Kerio Personal Firewall 4™

Uživatelský manuál

Kerio Technologies

Datum vydání: 29. června 2005

Tento manuál popisuje produkt *Kerio Personal Firewall* ve verzi *4.2.0*. Změny vyhrazeny.

Aktuální verzi produktu a manuálu naleznete na WWW stránkách `http://www.kerio.cz/kpf`.

Obsah

Kapitola 1

Úvod

1.1 Kerio Personal Firewall 4.2

Kerio Personal Firewall je aplikace určená k ochraně osobního počítače s operačním systémem Windows 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.

Blokování chování aplikací

Modul *Blokování chování aplikací* 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.x (narozdíl od starších verzí) kontroluje spouštění všech aplikací, bez ohledu na to, zda se účastní síťové komunikace. V případě virové nákazy 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 a prevence síťových útoků

Systém detekce a prevence síťových útoků (*NIPS — Network Intrusion Prevention 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).

Detekce a prevence útoků na hostitelský systém

Systém detekce a prevence útoků na hostitelský systém (HIPS — Host Intrusion Prevention System) zachycuje pokusy o zneužití spuštěných aplikací k provedení zákeřného kódu.

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).

Nízkoúrovňová ochrana

Nízkoúrovňový ovladač *Kerio Personal Firewallu* chrání počítač i v době, kdy není firewall spuštěn (typicky při startu a vypínání operačního systému a při instalaci nové verze firewallu). Počítač je tak chráněn po celou dobu, kdy je dostupný po síti.

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 typu Windows Server (tj. Windows NT Server, Windows 2000 Server a Windows Server 2003).

1.2 Systémové požadavky

Pro instalaci aplikace *Kerio Personal Firewall* je požadováno:

- operační systém Windows 2000 Professional / XP Home / XP Professional
- CPU Intel Pentium nebo 100% kompatibilní
- 64 MB RAM
- 8 MB místa na disku (pouze pro instalaci; doporučujeme nejméně dalších 10 MB pro soubory záznamů)
- rozlišení obrazovky (displeje) alespoň 800x600 bodů

1.3 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* (*Sdílení internetového připojení* — součást novějších verzí operačního systému Windows) za účelem vytvoření jednoduchého síťového firewallu. Podrobné informace najdete v kapitole 6.3.

Kapitola 2

Instalace

2.1 Instalace, upgrade a odinstalování

Instalace

Instalaci provedete jednoduše spuštěním instalačního programu — např.

```
kerio-pf-4.2.0-en-win.exe
```

Instalační program se nejprve dotáže na jazyk, ve kterém má být instalace provedena (k dispozici je angličtina a němčina). Volba jazyka se týká pouze instalace; uživatelské rozhraní aplikace *Kerio Personal Firewall* lze přepnout do několika dalších jazyků včetně češtiny (podrobnosti viz kapitola 6.3).

V dalším kroku lze zvolit adresář (složku), do kterého bude aplikace *Kerio Personal Firewall* nainstalována — standardně

```
C:\Program Files\Kerio\Personal Firewall 4
```

Dalším důležitým krokem při instalaci je volba výchozího režimu činnosti firewallu. Začínajícím uživatelům doporučujeme ponechat přednastavený režim *Simple*, zkušenější uživatelé mohou zvolit režim *Advanced* (chování v tomto režimu odpovídá chování předchozích verzí *Kerio Personal Firewallu*). Režim činnosti firewallu lze později libovolně změnit. Podrobnosti o výchozích režimech firewallu naleznete v kapitole 2.2.

Po instalaci je třeba počítač restartovat, aby mohl být zaveden nízkoúrovňový ovladač firewallu. Po restartu počítače bude automaticky spuštěna komponenta *Personal Firewall Engine* (viz kapitola 4.1)

Upozornění: Chcete-li používat *Kerio Personal Firewall* společně s antivirovým systémem *AVG*, je třeba *AVG* nainstalovat před zahájením instalace *Kerio Personal Firewallu*. Jestliže *Kerio Personal Firewall* při svém prvním spuštění detekuje antivirus *AVG*, nastaví pro něj odpovídající pravidla (viz kapitola 9.3).

Poznámky:

1. 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 6.3) se v operačním systému nastaví generování výpisu paměti také při pádu aplikace *Kerio Personal Firewall*.

2. *Kerio Personal Firewall* při svém startu vypíná integrovaný *Windows Firewall*, pokud je spuštěn.

   V operačních systémech Windows XP Service Pack 2 a novějších instalační program zaregistruje *Kerio Personal Firewall* do *Windows Security Center*. Při instalaci je firewall zaregistrován jako neaktivní.

3. V operačním systému Windows 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!

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 2.3).

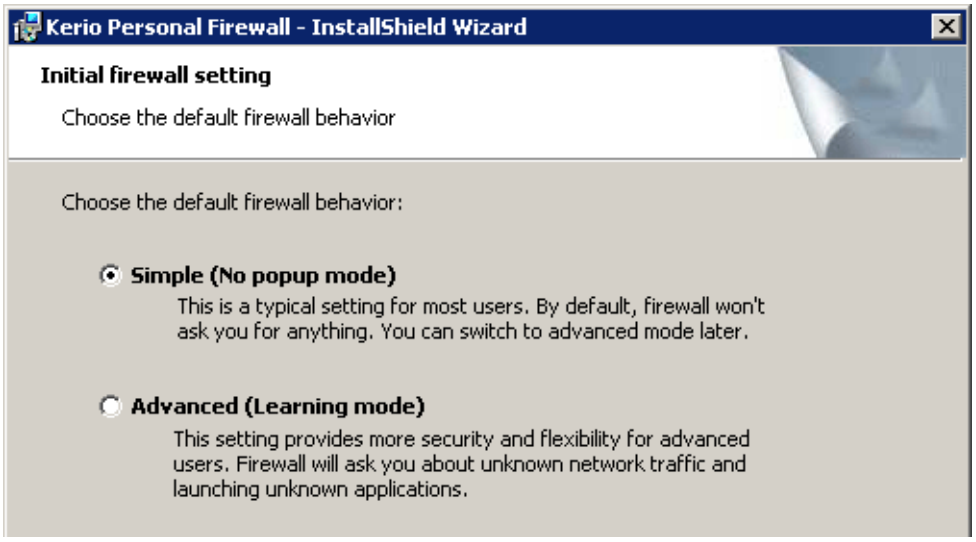
Odinstalování

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.). Tyto soubory můžeme po odinstalování aplikace smazat ručně, případně je můžeme uchovat pro další instalaci.

Poznámka: V operačních systémech Windows XP Service Pack 2 a novějších bude při odinstalování *Kerio Personal Firewallu* zrušena jeho registrace ve *Windows Security Center* a automaticky aktivován vestavěný *Windows Firewall*.

2.2 Počáteční konfigurace

Během instalace aplikace *Kerio Personal Firewall* lze zvolit tzv. výchozí režim činnosti firewallu. Uživatel může vybrat jeden z těchto režimů:



Obrázek 2.1 Volba výchozího chování firewallu (při instalaci)

- *Simple* — v tomto režimu firewall automaticky povoluje veškerou odchozí komunikaci a blokuje veškerou příchozí komunikaci. Všechna síťová rozhraní počítače, na kterém je *Kerio Personal Firewall* nainstalován, jsou automaticky zařazena do zóny *Internet* (viz kapitoly 7.2 a 7.4). Dále je vypnut modul bezpečnosti systému (viz kapitola 13).

  V důsledku těchto nastavení se firewall uživatele nikdy nedotazuje a pracuje výhradně podle výchozích pravidel (ve výchozích pravidlech se nikde nevyskytuje akce *Ptát se*). Toto chování firewallu lze změnit úpravou nastavení modulů systémové a síťové bezpečnosti.

  Poznámka: Výjimkou je kontrola telefonních čísel vytáčených linek (viz kapitola 7.8). Dialogy s dotazy na nové telefonní číslo nebo změnu telefonního čísla se zobrazují vždy bez ohledu na nastavený režim firewallu.

  Režim *Simple* je při instalaci přednastaven. Doporučujeme jej zejména začátečníkům, případně uživatelům, kteří z nějakého důvodu nemohou provést počáteční konfiguraci firewallu bezprostředně po instalaci.

- *Advanced* (tzv. samoučící režim) — v tomto režimu se firewall při zachycení neznámé komunikace nebo při spuštění neznámé aplikace dotazuje uživatele, jaká akce má být provedena a zda se má pro tuto akci vytvořit pravidlo. Takto postupně vzniká specifická konfigurace firewallu pro konkrétní počítač a uživatele.

  Je-li zvolen režim *Advanced*, pak *Kerio Personal Firewall* při svém prvním spuštění detekuje aktivní síťová rozhraní počítače, na kterém je nainstalován. Pro každé rozhraní zobrazí dotaz, zda je toto rozhraní připojeno do důvěryhodné sítě či nikoliv. Podrobnosti naleznete v kapitole 7.7.

  Režim *Advanced* nastavuje stejné výchozí chování *Kerio Personal Firewallu* jako všechny předchozí verze této aplikace. Tento režim doporučujeme zkušenějším uživatelům a všem uživatelům, kteří si chtějí firewall sami podrobně nastavit.

2.3 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 6.3).

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.

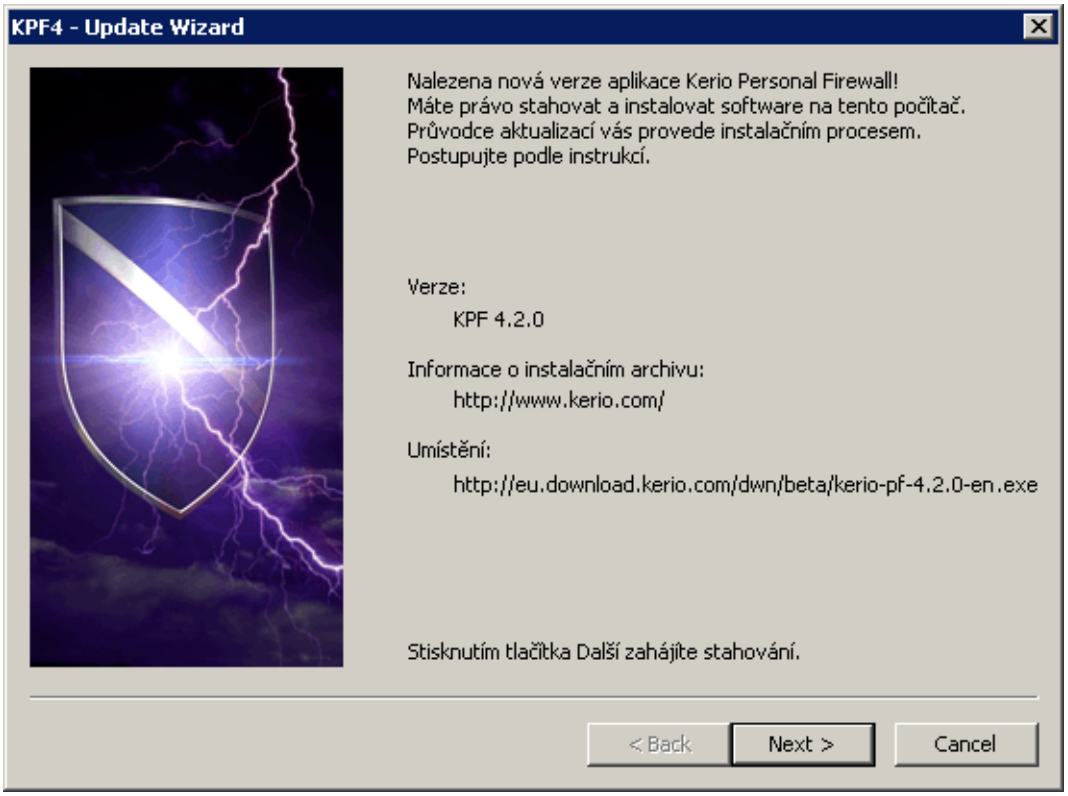
Stisknutím tlačítka *Další* se zahájí stahování nové verze. *Kerio Personal Firewall* vždy kontroluje signaturu staženého souboru — tím je zajištěno, že stažený soubor je skutečně originální (nejedná se o podvrh, není napaden virem, poškozen atd.).

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 2.1.

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.



Obrázek 2.2 Průvodce aktualizací produktu *Kerio Personal Firewall*

Kapitola 3

Registrace a licence produktu

3.1 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 kapitolu 3.2).

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 14).
- Není funkční systém prevence útoků na hostitelský operační systém (HIPS). Více najdete v kapitole 12.
- Nemůže být použita na internetové bráně (viz kapitola 6.3).
- Záznamy nelze odesílat na *Syslog* server (viz kapitola 16.3).
- 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.cz/`.

3.2 Registrace produktu

Zakoupenou licenci produktu *Kerio Personal Firewall* je třeba registrovat. Registrací se aktivují funkce, které nejsou ve volně šiřitelné verzi dostupné (viz kapitola 3.1).

Registraci *Kerio Personal Firewallu* lze provést přímo v uživatelském rozhraní firewallu, případně na WWW stránkách firmy *Kerio Technologies*.

Poznámky:

1. 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 3.1.

2. Podrobné informace o licenční politice naleznete na WWW stránkách firmy *Kerio Technologies* (`http://www.kerio.cz/`).

Registrace v uživatelském rozhraní

Má-li počítač s *Kerio Personal Firewallem* přímý přístup do Internetu, pak lze registraci provést přímo v uživatelském rozhraní firewallu.

K zobrazení informací o licenci a registraci licence a předplatného slouží záložka *Licence* v sekci *Přehled*. Podoba této záložky závisí na aktuální licenci a/nebo stavu produktu.

Neregistrovaná verze ve zkušební lhůtě

V tomto stavu se produkt nachází po dobu 30 dnů od první instalace na konkrétní počítač. V tomto období je produkt plně funkční i bez licence.
Sekce *Produkt* obsahuje základní informace o produktu. Tlačítko *Registrovat* spouští průvodce registrací (viz kapitola 3.3).
Sekce *Licence* zobrazuje počet dní zbývajících do konce zkušební doby.

Obrázek 3.1 Sekce *Přehled / Licence* — neregistrovaná verze ve zkušební lhůtě

Neregistrovaná verze po uplynutí zkušební doby

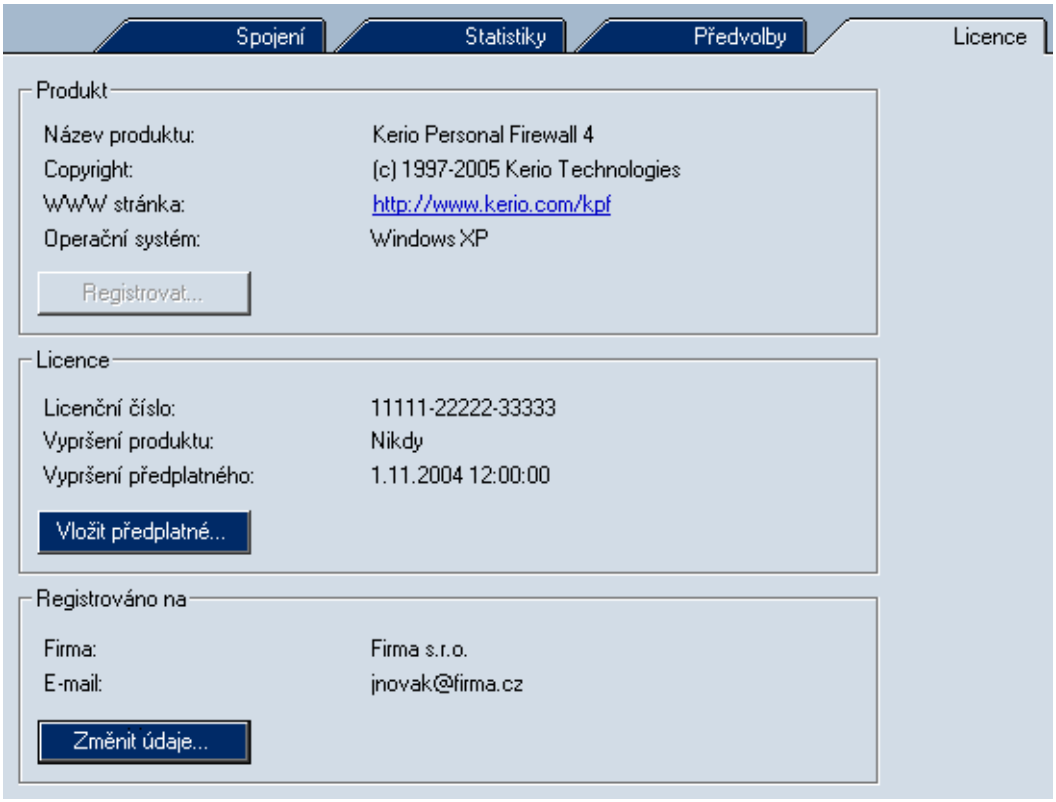
Tento stav nastává po uplynutí třicetidenní zkušební doby, pokud nebyl produkt dosud zaregistrován. Produkt přechází do režimu tzv. omezené verze, kdy jsou zablokovány některé funkce (podrobnosti viz kapitola 3.1).

Sekce *Produkt* umožňuje registraci produktu, stejně jako v předchozím případě. Sekce *Licence* informuje o tom, že produkt běží v režimu omezené neregistrované verze.

Obrázek 3.2 Sekce *Přehled / Licence* — neregistrovaná verze po uplynutí zkušební lhůty

Platná licence

Je-li *Kerio Personal Firewall* již zaregistrován, pak jsou dostupné všechny jeho funkce bez časového omezení. Záložka *Licence* pak zobrazuje podrobné informace o aktuální licenci.



Obrázek 3.3 Sekce *Přehled / Licence* — registrovaná verze

Tlačítko *Registrovat* v sekci *Produkt* je neaktivní.

Sekce *Licence* zobrazuje aktuální licenční číslo a data skončení funkčnosti produktu a skončení nároku na bezplatné aktualizace (předplatného). Tlačítko *Vložit předplatné* umožňuje zaregistrovat prodejní číslo zakoupeného předplatného na další období. Po stisknutí tohoto tlačítka se otevře průvodce registrací produktu od 3. kroku (viz kapitola 3.3).

V sekci *Registrováno na* lze změnit kontaktní údaje firmy nebo osoby, na kterou je produkt registrován. V jednotlivých položkách dialogu budou předvyplněny aktuální údaje získané z registračního serveru. Položky *Firma / Jméno a stát* nelze změnit (licenci nelze přeregistrovat na jiný subjekt).

Registrace na WWW stránkách

Produkt *Kerio Personal Firewall* lze zaregistrovat také na WWW stránkách firmy *Kerio Technologies* (`http://www.kerio.cz/`, sekce *Obchod / Registrace licencí*). Tento způsob registrace lze využít v případě, pokud není možné z počítače s aplikací *Kerio Personal Firewall* navázat spojení se serverem firmy *Kerio Technologies* (např. je-li komunikace blokována síťovým firewallem).

Do příslušného formuláře je třeba zadat registrační číslo získané při zakoupení produktu a následně čísla zakoupeného předplatného. Jsou-li všechna zadaná čísla platná, bude vytvořen odpovídající licenční klíč (soubor `license.key`). Tento soubor je třeba stáhnout a uložit do podadresáře `license` v adresáři, kde je *Kerio Personal Firewall* nainstalován

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

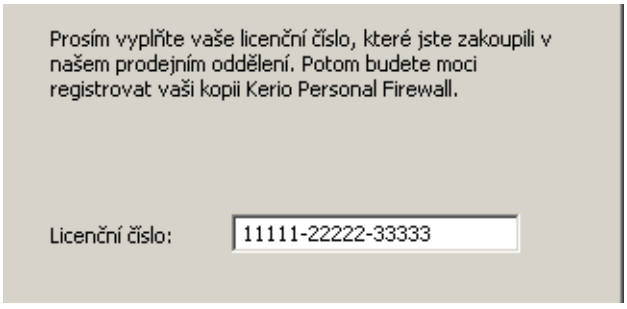
Po dalším spuštění služby *Personal Firewall Engine* se již bude produkt chovat jako plná verze.

3.3 Průvodce registrací produktu

Registrace produktu *Kerio Personal Firewall* probíhá ve čtyřech krocích:

Krok 1 — zadání licenčního čísla

V prvním kroku průvodce je třeba vyplnit licenční číslo získané při zakoupení produktu (*Licenční číslo*).



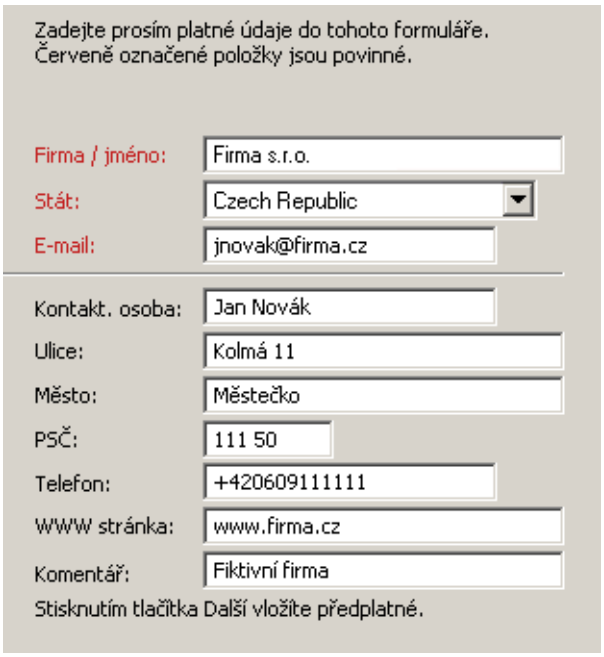
Obrázek 3.4 Průvodce registrací — zadání licenčního čísla (krok 1)

Po stisknutí tlačítka *Další* naváže *Kerio Personal Firewall* spojení s registračním serverem a zkontroluje platnost zadaného čísla. Je-li číslo neplatné, v registraci nelze pokračovat.

Nepodaří-li se navázat spojení s registračním serverem (počítač nemá přímý přístup na Internet, komunikace je blokována jiným firewallem apod.), pak je uživateli nabídnut odkaz pro registraci produktu na WWW stránkách firmy *Kerio Technologies*.

Krok 2 — kontaktní údaje

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



Obrázek 3.5 Průvodce registrací — údaje o zákazníkovi (krok 2)

Červeně označené 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.

Krok 3 — předplatné

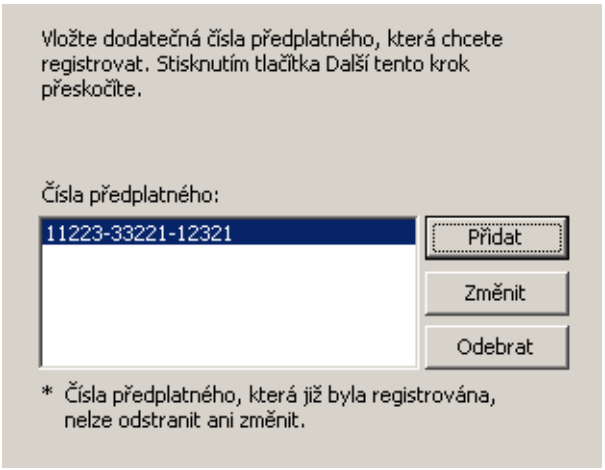
Třetí krok průvodce umožňuje zadat prodejní čísla zakoupeného předplatného na další období. Pokud máte zakoupenu pouze základní licenci (typicky při první registraci produktu), pak tento krok přeskočte.

Do pole *Čísla předplatného* lze přidat jedno nebo více prodejních čísel získaných při koupi předplatného. Přidaná čísla lze dle potřeby opravit nebo odstranit. Všechna čísla budou zaregistrována najednou po stisknutí tlačítka *Další*.

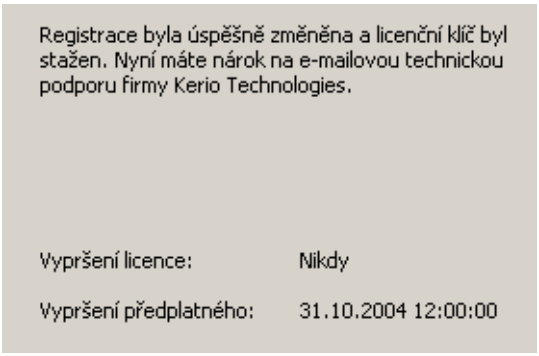
Po stisknutí tlačítka *Další* naváže *Kerio Personal Firewall* spojení s registračním serverem, ověří správnost zadaných údajů a automaticky stáhne licenční klíč (digitální certifikát).

Krok 4 — dokončení registrace

Ve čtvrtém kroku průvodce se zobrazí informace o výsledku registrace.



Obrázek 3.6 Průvodce registrací — zadání licenčních čísel předplatného (krok 3)



Obrázek 3.7 Průvodce registrací — informace o úspěšném provedení registrace a platnosti licence (krok 4)

Uživatel je informován o datu a čase vypršení předplatného (tj. nároku na bezplatné aktualizace produktu), a v případě časově omezené licence také o datu a čase skončení funkčnosti produktu (*Vypršení licence*).

Stisknutím tlačítka *Dokončit* se průvodce uzavře.

Poznámka: Po dokončení registrace se automaticky restartuje komponenta *Personal Firewall GUI*. Tím dojde k povolení všech funkcí, které nejsou v neregistrované verzi dostupné.

Kapitola 4

Komponenty firewallu a základní ovládání

4.1 Komponenty aplikace Kerio Personal Firewall

Personal Firewall Engine

Vlastní výkonné jádro *Kerio Personal Firewallu*. Běží jako systémová služba.

Služba *Personal Firewall Engine* je uložena v souboru `kpf4ss.exe` v instalačním adresáři aplikace *Kerio Personal Firewall*. Systémová služba má název `Kerio Personal Firewall 4` a zkrácený název `kpf4`.

Nízkoúrovňové ovladače

Zavádí se do jádra operačního systému při jeho startu. Jsou umístěny mezi ovladači síťových rozhraní a TCP/IP subsystémem.

Nízkoúrovňový ovladač pro kontrolu síťové komunikace

Nízkoúrovňový ovladač pro kontrolu síťové komunikace zachytává a zpracovává veškerou přijatou či vysílanou IP komunikaci. Tento nízkoúrovňový ovladač propouští a blokuje komunikaci podle nastavených pravidel firewallu a zároveň kontroluje spouštění aplikací v systému.

Nízkoúrovňový ovladač pro kontrolu útoků na hostitelský systém

Nízkoúrovňový ovladač pro kontrolu útoků na hostitelský systém kontroluje a případně blokuje (podle nastavení v uživatelském rozhraní) útoky typu *Přetečení vyrovnávací paměti* a *Injekce kódu*.

Oba nízkoúrovňové ovladače jsou uloženy v systémovém adresáři Windows:

- v operačním systému Windows 2000 typicky v adresáři `C:\WINNT\system32\drivers` (soubory `fwdrv.sys` a `khips.sys`)
- v operačním systému Windows XP typicky v adresáři `C:\WINDOWS\system32\drivers` (soubory `fwdrv.sys` a `khips.sys`)

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 oznamovací oblasti 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 4.2.

Obrázek 4.1 Ikona aplikace *Kerio Personal Firewall* v oznamovací oblasti nástrojové lišty

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

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`.

Knihovní moduly

Výše popsané komponenty aplikace *Kerio Personal Firewall* využívají pro svou činnost následující dynamické knihovny (DLL):

- `kfe.dll` — rozhraní nízkoúrovňového ovladače. Toto rozhraní zajišťuje komunikaci mezi ovladačem a *Personal Firewall Engine*.
- `gkh.dll` — modul pro obsluhu horkých kláves. Tento modul je zodpovědný za dočasné vypínání filtru pop-up oken.
- `kwsapi.dll` — rozhraní pro *Windows Security Center* (registrace *Kerio Personal Firewallu* a zobrazování jeho stavu).
- `KTssleay32_0.9.7.dll`, `libeay32_0.9.7.dll` — knihovna *OpenSSL*. Tato knihovna zajišťuje šifrování konfiguračních souborů a komunikace mezi *Personal Firewall GUI* a *Personal Firewall Engine*.
- `KTiconv.dll` — knihovna *iconv*. Tato knihovna provádí převod kódování znaků např. při filtrování WWW stránek, zápisu informací do záznamů atd.
- `KTzlib.dll` — knihovna *zlib*. Tato knihovna se používá pro komprimaci výpisů paměti.

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).

4.2 Ikona na nástrojové liště

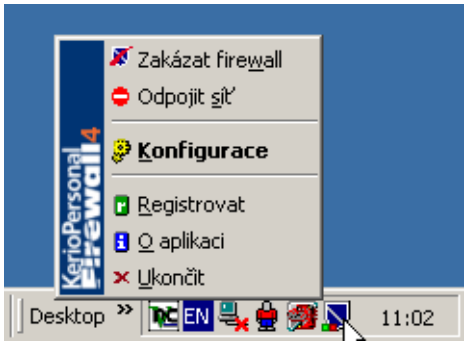
Ikona aplikace *Kerio Personal Firewall* v pravé části nástrojové lišty (System Tray) je zobrazena vždy, když běží komponenta *Personal Firewall GUI*. Tuto komponentu spouští automaticky služba *Personal Firewall Engine*.

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

Obrázek 4.2 Ikona aplikace *Kerio Personal Firewall* na nástrojové liště

- 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 6). Po kliknutí na ikonu pravým tlačítkem myši se zobrazí menu s těmito funkcemi:



Obrázek 4.3 Kontextové menu ikony na nástrojové liště

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.

Obrázek 4.4 Ikona aplikace *Kerio Personal Firewall* — firewall zakázán

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

Poznámka: V operačních systémech Windows XP Service Pack 2 je při zakázání nebo povolení *Kerio Personal Firewallu* nahlášen jeho aktuální stav do *Windows Security Center*.

Odpojit síť

Zablokování veškeré síťové komunikace (tzv. síťový zámek).

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

Obrázek 4.5 Ikona aplikace *Kerio Personal Firewall* — blokování síťové komunikace

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 7.2, resp. 8) 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

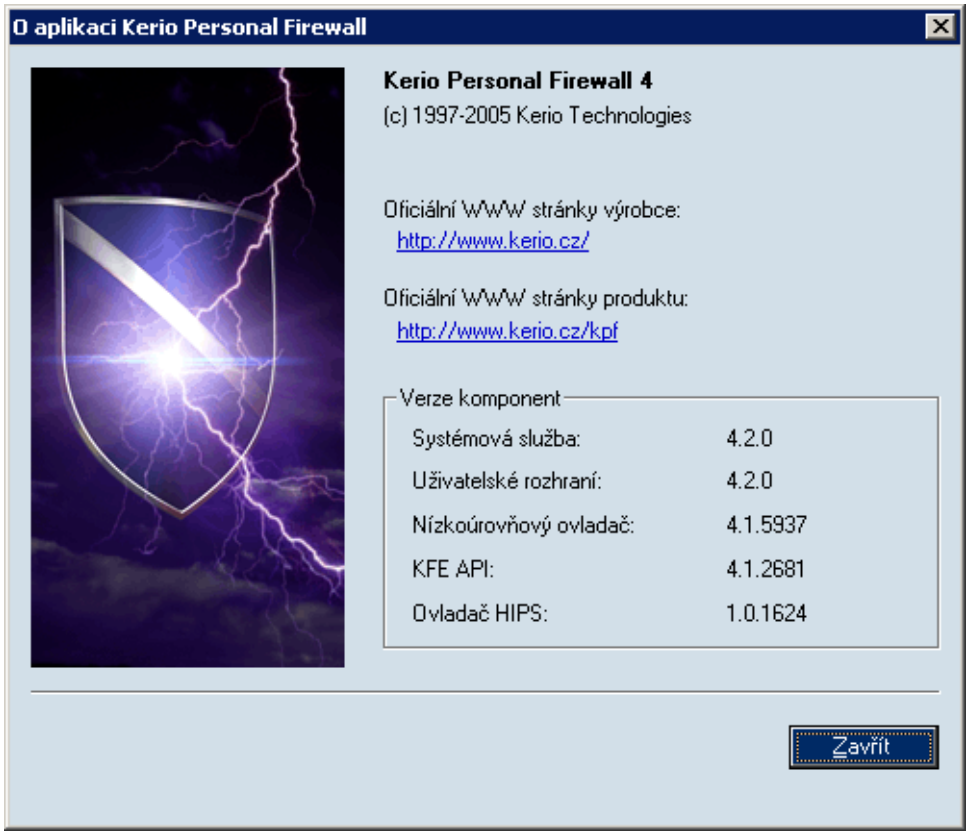
firewallu je detailně popsána v kapitole 6.

Registrovat

Spuštění průvodce registrací produktu (podrobnosti viz kapitola 3.2). 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 odkazy na WWW stránky výrobce aplikace.



Obrázek 4.6 Okno *O aplikaci*

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).

Kerio Personal Firewall lze znovu aktivovat volbou *Firewall Engine* z nabídky *Start* → *Programy* → *Kerio* → *Personal Firewall 4*, případně spuštěním služby v ovládacím panelu *Nástroje pro správu / Služby* (*Administrative Tools / Services*).

Upozornění: Po ukončení aplikace *Kerio Personal Firewall* začne nízkoúrovňový ovladač automaticky povolovat veškerou odchozí i příchozí komunikaci — počítač přestává být chráněn! Podrobnosti viz kapitola 7.6.

Je-li přístup ke správě firewallu chráněn heslem a uživatel je přihlášen, pak je kontextové menu rozšířeno o položku *Odhlásit*. Bližší informace naleznete v kapitole 6.2.

Kapitola 5

Chování firewallu a interakce s uživatelem

5.1 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. Firewall při svém rozhodování nepracuje pouze s informacemi ze zachyceného paketu, ale také s informací o stavu předchozí komunikace. O každém povoleném spojení (resp. pseudospojení v případě protokolů UDP a ICMP) je vytvořen záznam. Firewall tak dokáže přesně určit, zda zachycený paket patří do povoleného spojení, a podle toho jej propustí nebo blokuje. Stavová inspekce síťové komunikace je několikanásobně účinnější a bezpečnější než samotné filtrování paketů.

Je-li při instalaci *Kerio Personal Firewallu* zvolen režim *Advanced* (viz kapitola 2.2), pak firewall pracuje v tzv. samoučícím módu. 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 5.2 a 8.

Poznámka: Obdobným způsobem *Kerio Personal Firewall* postupuje také při kontrole spouštěných aplikací (podrobnosti viz kapitola 13.2).

Úpravou pravidel pro aplikace nebo pravidly rozšířeného paketového filtru může uživatel (resp. administrátor) specifikovat další podmínky pro filtrování komunikace. Vždy jsou ale propuštěny jen takové pakety, které jsou povoleny příslušnými pravidly nebo patří do povolených spojení (viz stavová inspekce).

Upozorňující dialogy jsou zobrazeny vždy nad okny ostatních aplikací („Always on Top“). Je-li zachyceno více událostí (tj. více pokusů o navázání spojení, spuštění aplikací,

pokusů o útok, atd.) současně, pak se tyto události řadí do fronty — teprve po potvrzení jednoho dialogu se zobrazí další; nikdy se nezobrazuje více dialogů současně.

5.2 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 7.2 a 7.3). Dialog *Upozornění na spojení* se zobrazuje v případech, kdy neexistuje odpovídající pravidlo nebo pravidlo explicitně vyžaduje dotázat se uživatele.

Upozornění: V případě, že je konfigurace *Kerio Personal Firewallu* chráněna heslem (kapitola 6.3), lze v dialogu jednorázově povolit spojení, avšak bez zadání hesla není možné vytvořit pro toto spojení příslušné pravidlo.

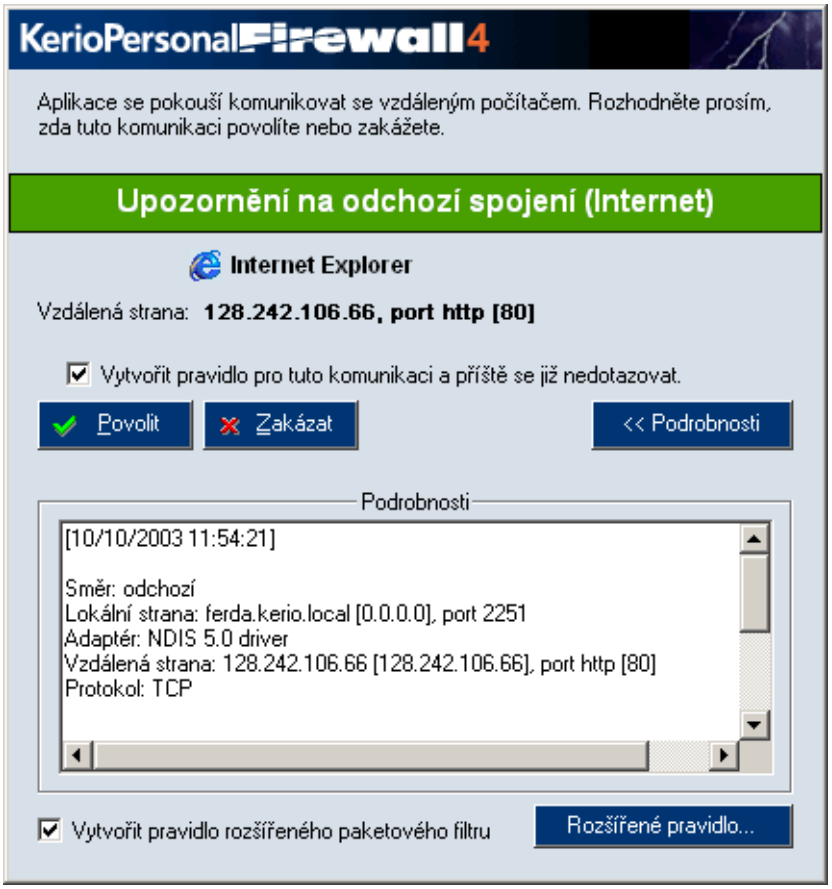
Dialog *Upozornění na spojení* obsahuje následující informace a volby:

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.



Obrázek 5.1 Dialog Upozornění na spojení (zachycení neznámé komunikace)

Obrázek 5.2 Dialog Upozornění na spojení — směr komunikace a zóna

- *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 7.4)
- *Internet* — „zbytek světa“ (tj. libovolná IP adresa, která nepatří do skupiny *Důvěryhodná zóna*)

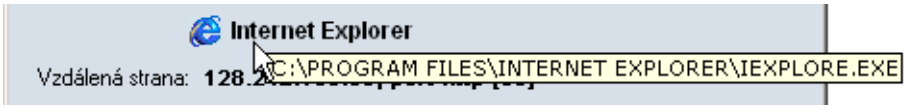
Lokální aplikace a vzdálený konec spojení

Pod barevným pruhem s informací o směru komunikace jsou uvedeny stručné informace o navazovaném spojení:

Obrázek 5.3 Dialog Upozornění na spojení — lokální aplikace a vzdálený konec 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 15.1)
- vzdálený port (jedná-li se o standardní službu, zobrazí se její jméno a číslo portu v hranatých závorkách; jinak číslo portu bez závorek)

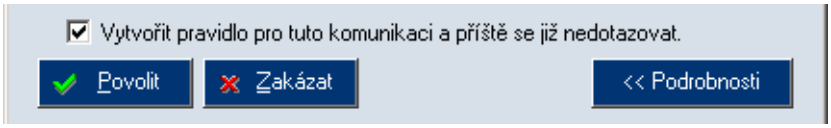
Při umístění kurzoru myši na popis aplikace se jako nápovědný text (tooltip) zobrazí úplná cesta k spustitelnému souboru aplikace.



Obrázek 5.4 Dialog Upozornění na spojení — zobrazení úplné cesty k aplikaci

Volba akce

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



Obrázek 5.5 Dialog Upozornění na spojení — volba akce

- 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

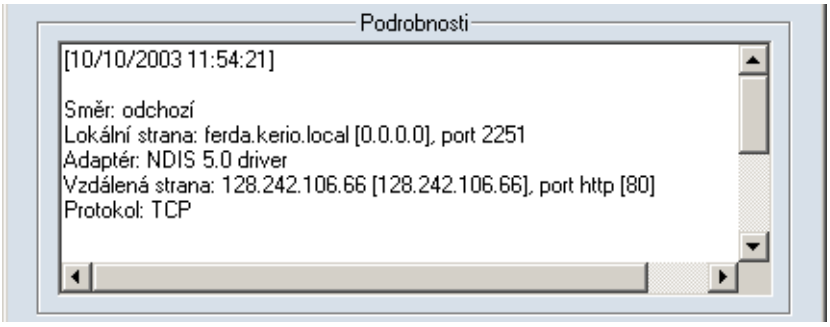
nebo odstranit v konfiguračním okně *Kerio Personal Firewallu* v sekci *Síťová bezpečnost*, záložka *Aplikace*. Podrobnosti naleznete v kapitole 7.2.

- 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*.

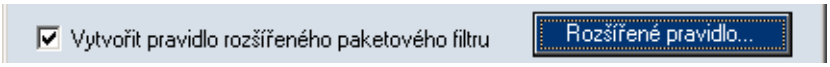
Detailní informace o spojení a lokální aplikaci

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).



Obrázek 5.6 Dialog Upozornění na spojení — detailní informace o spojení a lokální aplikaci

Vytvoření rozšířeného pravidla



Obrázek 5.7 Dialog Upozornění na spojení — vytvoření pravidla paketového filtru

Zaškrtnutím volby *Vytvořit pravidlo rozšířeného paketového filtru* bude namísto standardního pravidla pro aplikaci (viz kapitola 7.2) 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 8.

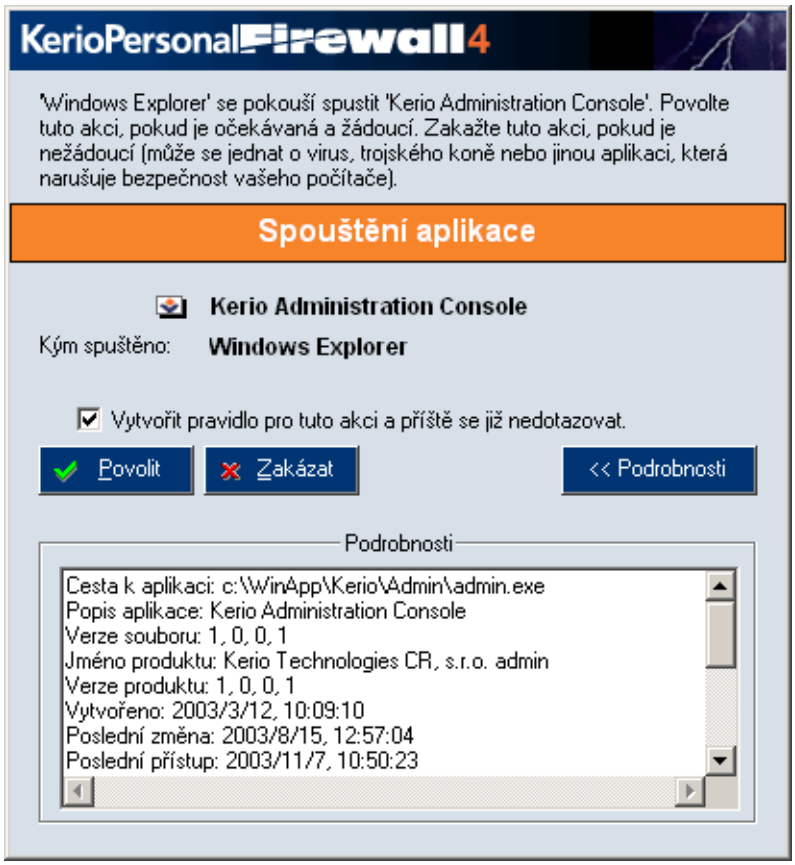
Poznámka: Po dobu, kdy je zobrazen dialog *Upozornění na spojení*, je příslušná komunikace „pozastavena“ (již přijatá či vyslaná data uchovává *Kerio Personal Firewall* ve své vyrovnávací paměti). Není-li reakce uživatele dostatečně rychlá, může vysílající aplikace po určité době (zpravidla několik desítek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

5.3 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 13). Dialog *Spouštění/Záměna/Spouštění jiné aplikace* se zobrazuje v případech, kdy neexistuje odpovídající pravidlo nebo pravidlo explicitně vyžaduje dotázat se uživatele.

Upozornění: V případě, že je konfigurace *Kerio Personal Firewallu* chráněna heslem (kapitola 6.3), lze povolit akci pouze po jeho správném zadání.

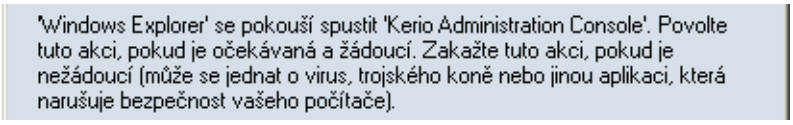


Obrázek 5.8 Dialog Spouštění/Záměna/Spouštění jiné aplikace

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.



Obrázek 5.9 Dialog Spouštění/Záměna/Spouštění jiné aplikace — popis události

Poznámka: Je-li popis aplikace (případně jméno souboru, pokud není popis k dispozici) příliš dlouhý, zkrátí se na 32 znaků a ukončí třemi tečkami.

Název události

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

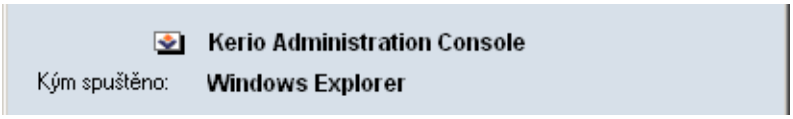
Obrázek 5.10 Dialog Spouštění/Záměna/Spouštění jiné aplikace — událost

- *Spouštění aplikace*
- *Záměna aplikace* — spustitelný souboru aplikace byl od posledního spuštění změněn
- *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.



Obrázek 5.11 Dialog Spouštění/Záměna/Spouštění jiné aplikace — ikona a popis 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.

Obrázek 5.12 Dialog Spouštění/Záměna/Spouštění jiné aplikace — zobrazení úplné cesty k aplikaci

Volba akce

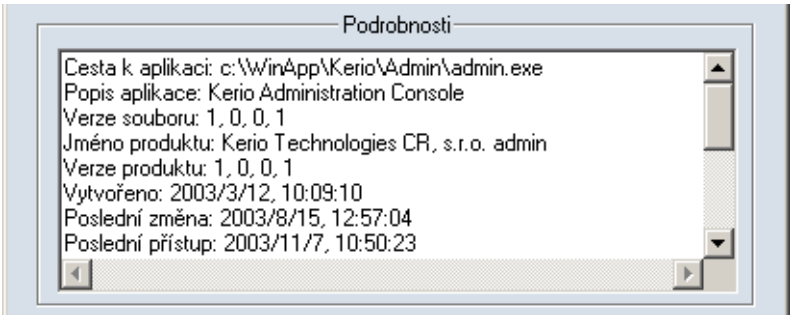
Nejdůležitější částí dialogu je volba akce — tedy povolení či zakázání spuštění příslušné aplikace.

Obrázek 5.13 Dialog Spouštění/Záměna/Spouštění jiné aplikace — volba akce

- 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.).

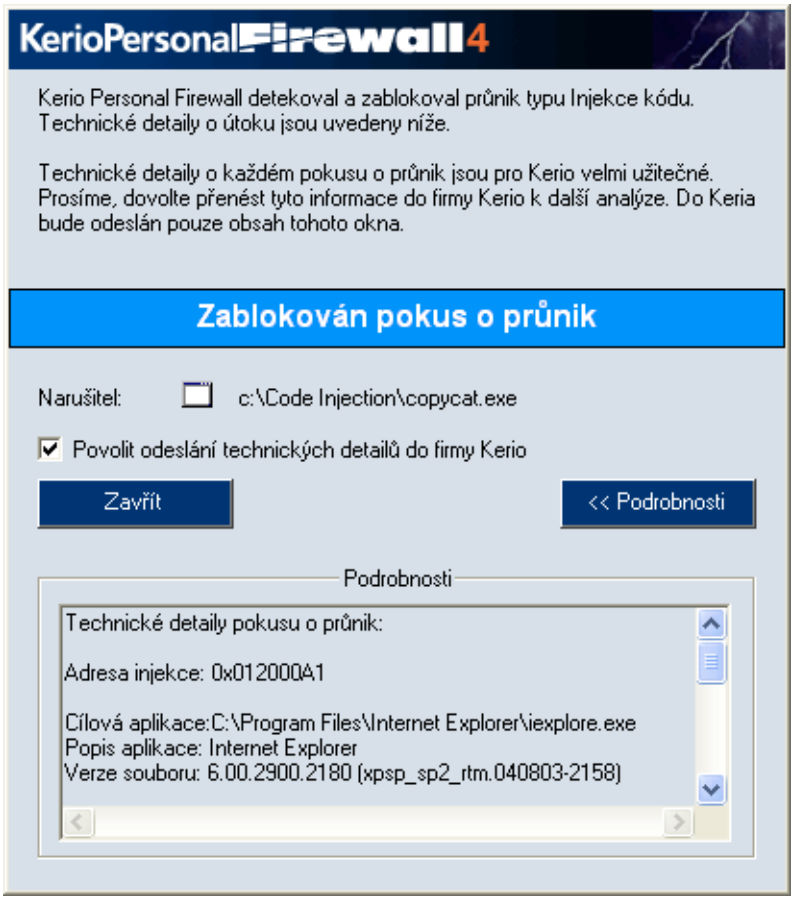


Obrázek 5.14 Dialog Spouštění/Záměna/Spouštění jiné aplikace — podrobnosti o aplikacích

5.4 Upozornění na útoky na hostitelský operační systém

Dialog *Zablokován pokus o útok* upozorňuje uživatele na to, že *Kerio Personal Firewall* detekoval pokus o útok na hostitelský operační systém a zablokoval ho.

Poznámka: Chování *Kerio Personal Firewallu* při detekování těchto typů útoků lze nastavit v kapitole 12). Dialog *Zablokován pokus o útok* se zobrazuje v případech, kdy na aplikace neexistuje odpovídající výjimka nebo pokud je vypnuta volba *Nezobrazovat žádná upozornění na události tohoto typu* (více viz kapitolu 12).



Obrázek 5.15 Dialog detekce pokusu o útok na hostitelský systém

Popis události

V záhlaví dialogového okna je uveden slovní popis zachyceného útoku a obecné doporučení, jakou akci by měl uživatel zvolit.

Název události

Bledě modrý pruh obsahuje informaci o tom, že byl zachycen pokus o průnik do hostitelského systému. Může se jednat o dva typy útoků:

- *Přetečení vyrovnávací paměti* — o tomto typu útoku se dozvíte více v kapitole 12.
- *Injekce kódu* — tento typ útoku podrobně popisuje kapitola 12.

Ikona a cesty k aplikacím

Pod informací o typu útoku je zobrazen popis a ikony napadající i napadené aplikace (viz obrázek 5.16). Nemá-li aplikace svoji ikonu, použije se standardní systémová ikona pro spustitelné soubory.

Obrázek 5.16 Detekce injekce kódu — Ikony a popis útoku

V případě útoku typu *Přetečení vyrovnávací paměti* se zobrazuje pouze proces, ve kterém došlo k tomuto typu útoku (viz obrázek 5.17).

Obrázek 5.17 Detekce přetečení vyrovnávací paměti — Ikona a popis procesu

Povolení odeslání informací pokusu o útok

Volba *Povolit odeslání technických detailů do firmy Kerio* je standardně zaškrtnuta a umožňuje specialistům firmy další vývoj detekce těchto typů útoků. Do firmy *Kerio Technologies* bude odeslán pouze obsah upozorňujícího dialogu.

Zavřít

Tlačítko slouží k zavření upozorňujícího dialogu. Po zavření doporučujeme zjistit v záznamu HIPS podrobnosti o útoku (viz kapitolu 16.6).

Podrobnosti o útoku

Tlačítko *Podrobnosti* zobrazuje/skrývá podrobné informace o napadající i napadené aplikaci (v případě útoku typu *Přetečení vyrovnávací paměti* pouze o procesu) — úplnou cestu ke spustitelnému souboru, popis aplikace, číslo verze, atd.

5.5 Upozornění na událost

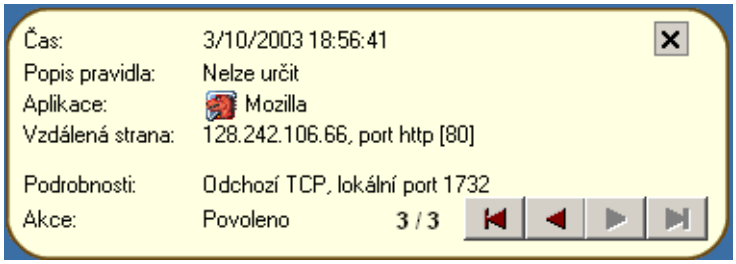
V pravidlech *Kerio Personal Firewallu* může být nastaveno zobrazení upozornění při zachycení komunikace vyhovující tomuto pravidlu, resp. při spuštění odpovídající aplikace. Jestliže *Kerio Personal Firewall* zaznamená takovou událost, zobrazí v pravém dolním rohu obrazovky okno s detailními informacemi. 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 obsahuje tyto položky:

- *Čas* — datum a čas, kdy událost nastala

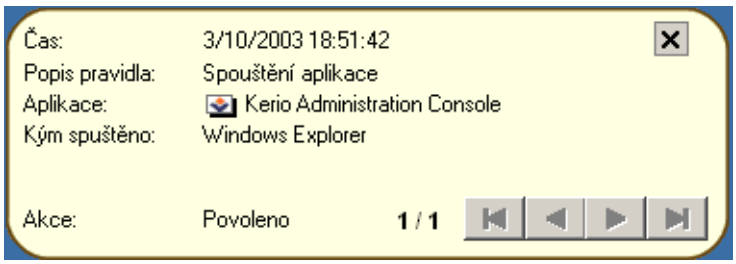


Obrázek 5.18 Upozornění na síťovou komunikaci

- *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 7.2.

Příklad upozornění na spouštění aplikace



Obrázek 5.19 Upozornění na spouštění aplikace

Upozornění 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) nebo *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 13.2.

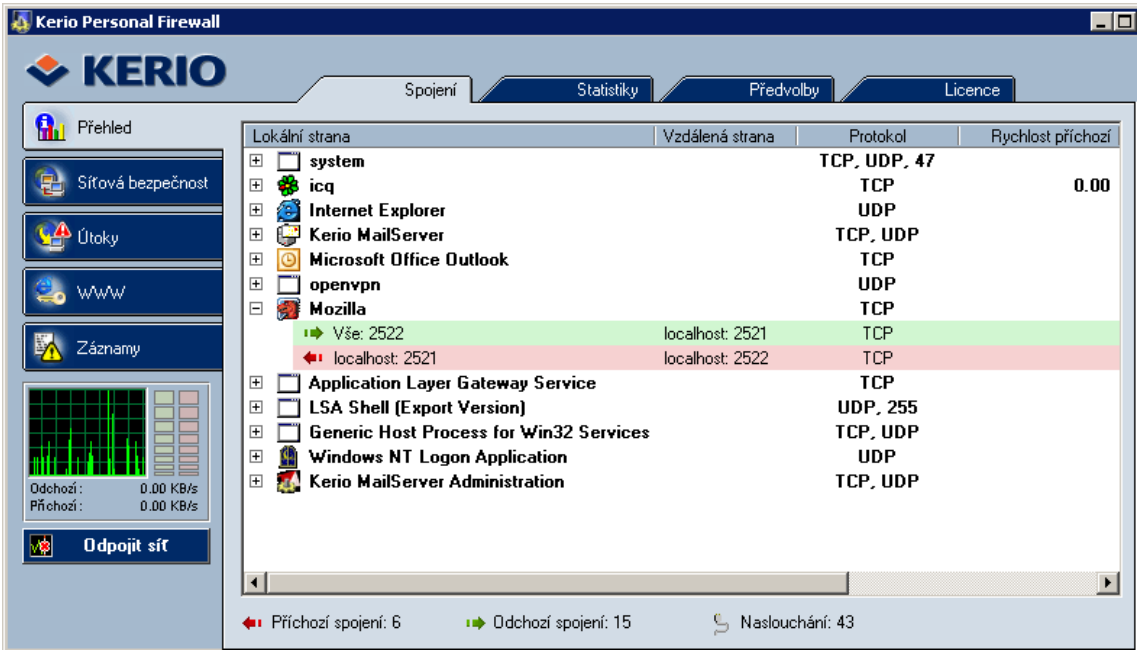
Kapitola 6

Konfigurace firewallu

6.1 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



Obrázek 6.1 Konfigurační okno aplikace *Kerio Personal Firewall*

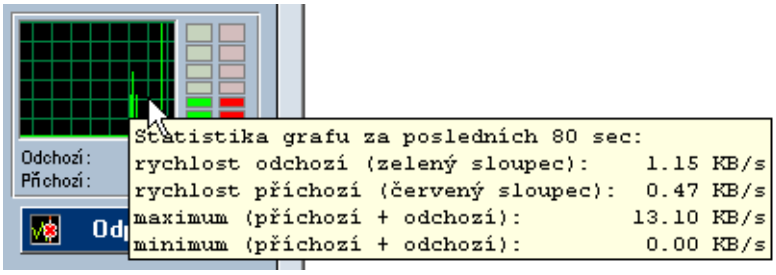
Záložky v levé části okna slouží k přepínání jednotlivých sekcí:

- *Přehled* — přehled aktivních spojení a otevřených portů (viz kapitola 15.1), statistiky (viz kapitola 15.2) a uživatelské preference (viz kapitola 6.3).
- *Síťová bezpečnost* — pravidla pro síťovou komunikaci aplikací, paketový filtr, definice důvěryhodné zóny (viz kapitola 7)
- *Bezpečnost systému* — pravidla pro spouštění aplikací (viz kapitola 13)
- *Útoky* — nastavení detekce známých typů útoků (viz kapitola 11)
- *WWW* — pravidla pro WWW stránky — blokování pop-up oken, URL filtr, blokování objektů, kontrola nad odesílanými daty (viz kapitola 14)
- *Záznamy* — prohlížení a nastavení záznamů (viz kapitola 16)

Graf v levé dolní části okna zobrazuje časový průběh zatížení síťového rozhraní (má-li počítač více síťových rozhraní, pak se statistiky za všechna rozhraní sčítají). 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 plošný graf.

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



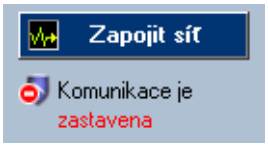
Obrázek 6.2 Konfigurační okno — časový průběh zatížení síťového rozhraní

- *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*.



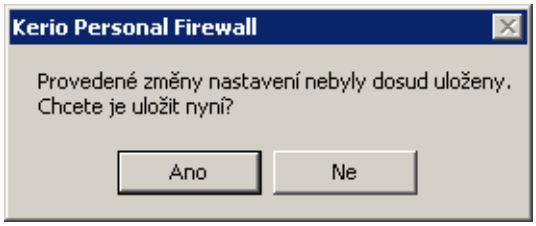
Obrázek 6.3 Konfigurační okno — blokování / povolení veškeré síťové komunikace

Poznámka: Volba *Odpojit síť / Zapojit síť* je dostupná také z kontextového menu ikony *Kerio Personal Firewallu* na nástrojové liště (viz kapitola 4.2).

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.

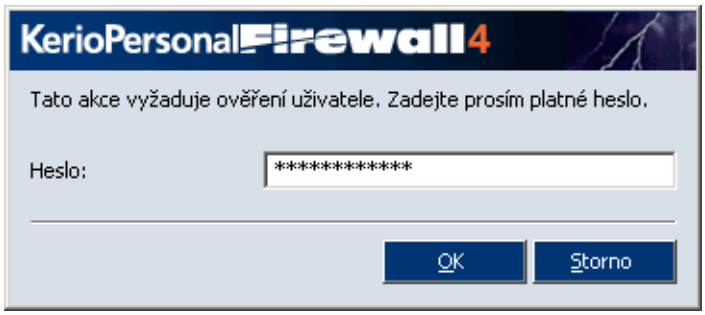


Obrázek 6.4 Konfigurační okno — dotaz na uložení provedených změn

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 6.3).

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



Obrázek 6.5 Ověření uživatele k provedení změny v konfiguraci

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 4.2), případně tlačítkem *Odhlásit* v sekci *Přehled / Předvolby*. Pokud se uživatel neodhlásí, je přihlášení platné až do ukončení běhu služby *Personal Firewall Engine*.

6.2 Vzdálená správa aplikace Kerio Personal Firewall

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. Povolení vzdálené správy a nastavení hesla

   Vzdálené připojení k *Personal Firewall Engine* je možné pouze na základě ověření uživatele heslem. V sekci *Přehled / Předvolby* zapněte volby *Povolit ochranu heslem* a *Povolit vzdálenou správu tohoto počítače*. Pokud nebylo dosud definováno heslo, nastavte jej. Podrobnosti naleznete v kapitole 6.3.

2. Spuštění *Personal Firewall GUI* na vzdáleném počítači

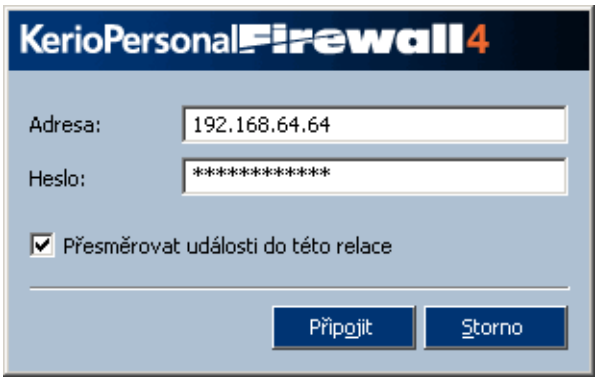
   - Je-li na vzdáleném počítači nainstalován *Kerio Personal Firewall 4.x*, spusťte komponentu *Remote Firewall Administration* z programové skupiny *Kerio*.

   - 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 soubory `kpf4gui.exe`, `KTlibeay32_0.9.7.dll`, `KTssleay32_0.9.7.dll`, `KTzlib.dll` 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*.



Obrázek 6.6 Připojení k *Personal Firewall Engine* na vzdáleném počítači

Adresa

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

- v záhlaví konfiguračního okna

Obrázek 6.7 Vzdálená správa — záhlaví konfiguračního okna

- v nápovědném textu (tooltip) ikony na nástrojové liště

Obrázek 6.8 Vzdálená správa — ikona 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.

Vzdálená správa

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:

Obrázek 6.9 Vzdálená správa — kontextové menu ikony na nástrojové liště

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 odpojení sítě). Podrobnosti viz kapitola 6.1.

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.

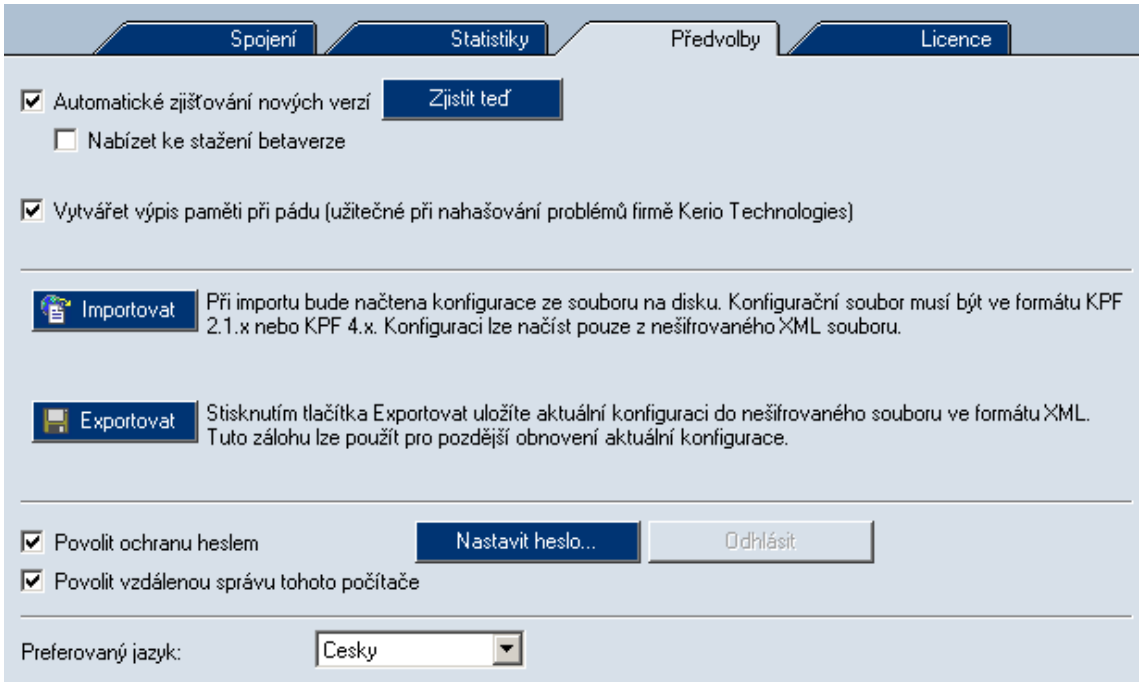
Narozdíl od lokální správy nejsou při vzdáleném připojení v kontextovém menu dostupné tyto funkce:

- *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*).

6.3 Předvolby

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

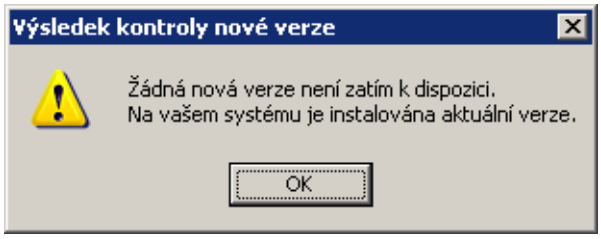
Automatické zjišťování nových verzí
Zapnutí/vypnutí automatické kontroly nových verzí programu. Pro zajištění maximální bezpečnosti doporučujeme ponechat tuto volbu zapnutou (nové verze obsahují aktualizace databáze známých útoků, opravy případných chyb atd.).
Podrobnosti o automatické kontrole a instalaci nové verze naleznete v kapitole 2.3.



Obrázek 6.10 Sekce *Přehled / Předvolby*

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 2.3). V opačném případě se zobrazí informace o tom, že novější verze není k dispozici (instalovaná verze je aktuální).



Obrázek 6.11 Kontrola nové verze — žádná nová verze není k dispozici

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.

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. 1 minutu po startu služby *Personal Firewall Engine* se provede kontrola, zda se na disku nenalézá nový výpis paměti. Je-li nalezen, spustí se nástroj *Assist*, který zkontroluje, zda tento výpis souvisí s pádem aplikace *Kerio Personal Firewall*. Pokud ano, nabídne se jeho odeslání do firmy *Kerio Technologies* k analýze.

Výpis paměti je odesílán v komprimované podobě. Do balíku je připojen také obsah větve systémového registru
`HKEY_CURRENT_USER\Software\Kerio\Personal Firewall 4`.

Poznámka:

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

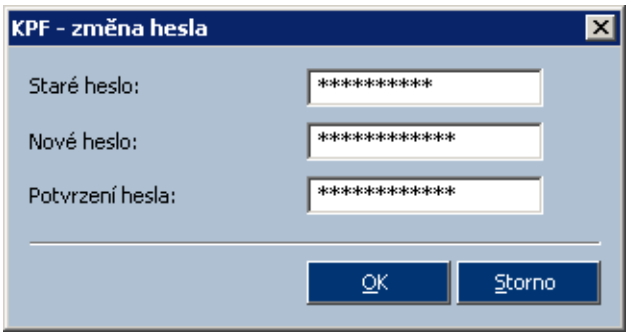
Poznámka: Konfigurační soubor verze *4.x* nelze v šifrované podobě importovat.

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 6.1.

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 4.2)

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



Obrázek 6.12 Nastavení hesla pro ochranu konfigurace

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 nelze ani povolit vzdálenou správu (následující volba je neaktivní).

Povolit vzdálenou správu tohoto počítače

Tato volba povoluje interní pravidlo firewallu připojení ke správě *Kerio Personal Firewallu* z jiného počítače (viz kapitola 9.1). Ve výchozím nastavení je vzdálená správa zakázána.

Podrobné informace o vzdálené správě naleznete v kapitole 6.2.

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.

Podle zvoleného jazyka se také vybírá nejvhodnější soubor s nápovědou. Není-li nalezena žádná preferovaná nápověda pro zvolený jazyk, pak *Kerio Personal Firewall* zkusí otevřít nápovědu v angličtině. Pokud není k dispozici ani anglická verze, nápověda se nezobrazí.

Poznámky:

1. Soubory s nápovědou jsou uloženy přímo v adresáři, kde je *Kerio Personal Firewall* nainstalován. Soubory s kontextovou nápovědou mají formát *Microsoft HTML Help* a mají název `kpf4-<zkratka_jazyka>.chm`, kde `zkratka_jazyka` je dvoupísmenné označení jazyka.

2. Pokud *Kerio Personal Firewall* zjistí, že lokalizační soubor pro vybraný jazyk neodpovídá aktuální verzi uživatelského rozhraní, zobrazí se varovné hlášení. Tento stav nemá žádný vliv na funkci programu, pouze některé texty v uživatelském rozhraní budou neaktuální nebo budou zobrazeny v anglickém originále.

Kapitola 7

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 7.2.

- *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 5.2)

  Nastavení rozšířeného paketového filtru je popsáno v kapitole 8.

- *Předdefinovaná pravidla pro síťovou komunikaci* — *Kerio Personal Firewall* obsahuje sadu předdefinovaných 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 7.3.

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.

7.1 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 kapitolu 11),

2. Stavová inspekce síťové komunikace (automatické propuštění paketů patřících do povolených spojení — viz kapitola 5.1),

3. Interní pravidla pro komponenty *Kerio Personal Firewallu* — např. povolení přístupu na WWW server firmy *Kerio Technologies* pro kontrolu a stahování nových verzí programu,

4. Pravidla rozšířeného paketového filtru (viz kapitola 8),

5. Předdefinovaná pravidla pro síťovou komunikaci (viz kapitola 7.3),

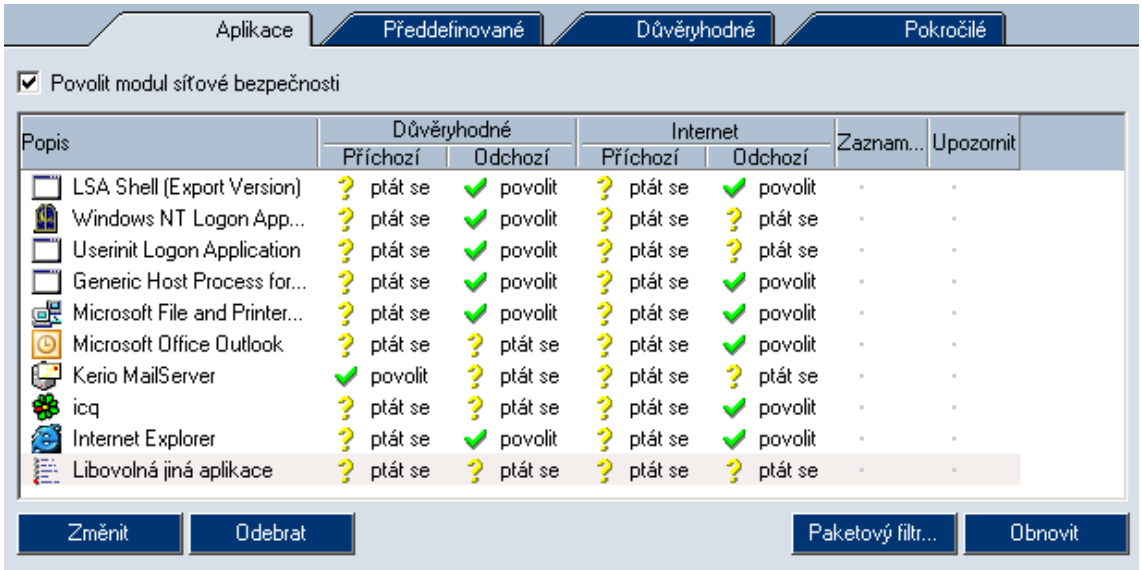
6. Pravidla pro síťovou komunikaci aplikací (viz kapitola 7.2).

Poznámka: Je-li vypnut modul síťové bezpečnosti a/nebo detekce útoků (viz kapitola 11), pak se příslušná pravidla na zachycenou komunikaci neaplikují. Interní pravidla firewallu vypnout nelze.

7.2 Pravidla pro aplikace

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

Poznámka: Následující informace platí pro případ, kdy *Kerio Personal Firewall* pracuje v režimu *Advanced* (viz kapitola 2.2). V režimu *Simple* je pro důvěryhodnou zónu i pro Internet všem aplikacím povolena odchozí komunikace a zakázána příchozí komunikace a žádná nová pravidla se automaticky nevytvářejí.



Obrázek 7.1 Sekce *Síťová bezpečnost / Aplikace* — pravidla pro síťovou komunikaci aplikací

Pro každou aplikaci může být definováno nejvýše jedno pravidlo. Na pořadí pravidel nezáleží.

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

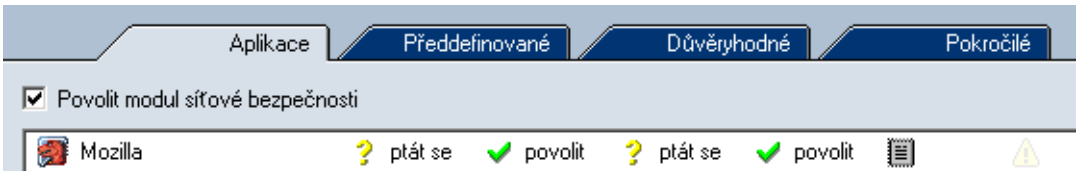
Nastavení chování firewallu při komunikaci dané aplikace s počítačem v důvěryhodné zóně a v Internetu v každém směru (*Příchozí*, *Odchozí*).

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 5.2) 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*



Obrázek 7.2 Pravidla pro aplikace — pravidlo pro WWW prohlížeč Mozilla

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 16.4), 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 5.5). 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).

Implicitní pravidlo

Na posledním místě seznamu pravidel pro síťovou komunikaci aplikací se vždy nachází pravidlo *Libovolná jiná aplikace* (tzv. implicitní pravidlo). Toto pravidlo se uplatňuje pro síťovou komunikaci aplikací, pro které neexistuje jiné pravidlo.

Implicitní pravidlo je v seznamu pravidel barevně zvýrazněno. Toto pravidlo nelze odstranit.

Poznámky:

1. Nastavením akcí v pravidle *Libovolná jiná aplikace* lze změnit režim činnosti firewallu (viz kapitola 2.2):

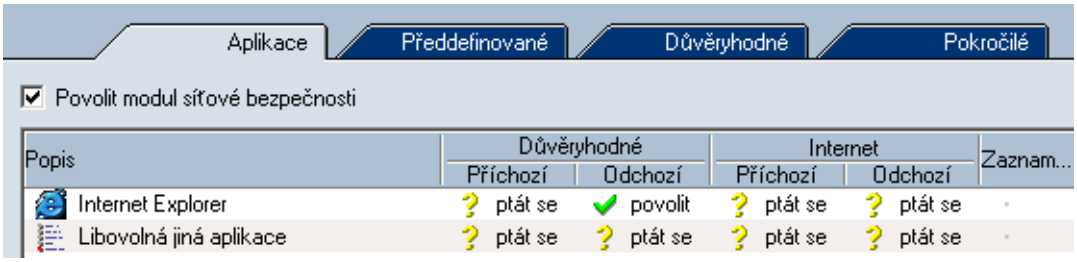
   - Je-li v tomto pravidle alespoň jedna akce *ptát se*, pak firewall pracuje v režimu *Advanced* — při zachycení dosud neznámé síťové komunikace se dotáže uživatele; na základě jeho reakce komunikaci povolí nebo zakáže, případně vytvoří pravidlo pro příslušnou aplikaci.

   - Jsou-li v pravidle *Libovolná jiná aplikace* pro obě zóny a oba směry komunikace nastaveny akce *povolit* nebo *zakázat*, pak firewall pracuje v režimu *Simple* — při zachycení neznámé komunikace je jednoznačně určeno, jaká akce má být provedena. V tomto případě se firewall uživatele nedotazuje.

2. Výchozí pravidlo je zároveň „šablonou“ pro nová pravidla vytvářená automaticky na základě interakce s uživatelem. Akce zvolená uživatelem se z bezpečnostních důvodů nastaví vždy pouze pro zónu a směr odpovídající zachycené komunikaci. Zbývající akce jsou převzaty z implicitního pravidla.

   Příklad: V implicitním pravidle je pro všechny zóny a směry komunikace nastavena akce *ptát se*. Uživatel spustí WWW prohlížeč *Microsoft Internet Explorer* a přistupuje

na server v lokální síti, která patří do důvěryhodné zóny. Firewall zobrazí dotaz na neznámou komunikaci (viz kapitola 5.2). Uživatel komunikaci povolí a požaduje vytvoření pravidla. Ve vytvořeném pravidle bude pro odchozí komunikaci v důvěryhodné zóně nastavena akce *povolit*, pro příchozí komunikaci v důvěryhodné zóně a pro oba směry v zóně *Internet* bude nastavena akce *ptát se* (převzatá z implicitního pravidla).



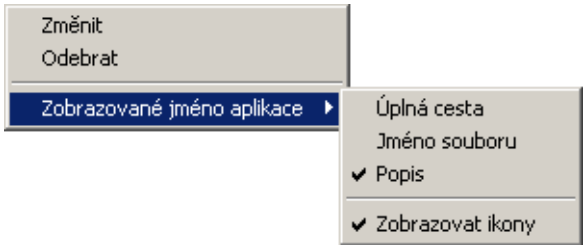
Obrázek 7.3 Pravidla pro aplikace — implicitní pravidlo a vytvořené pravidlo pro WWW prohlížeč

Výše popsané chování je třeba mít na paměti při nastavování akcí v implicitním pravidle. Obecně se doporučuje nastavit pro všechny zóny a směry komunikace akci *ptát se* (samoučící režim) nebo *zakázat* (blokování neznámé komunikace bez dotazování uživatele).

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:



Obrázek 7.4 Pravidla pro aplikace — kontextové menu

- *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.

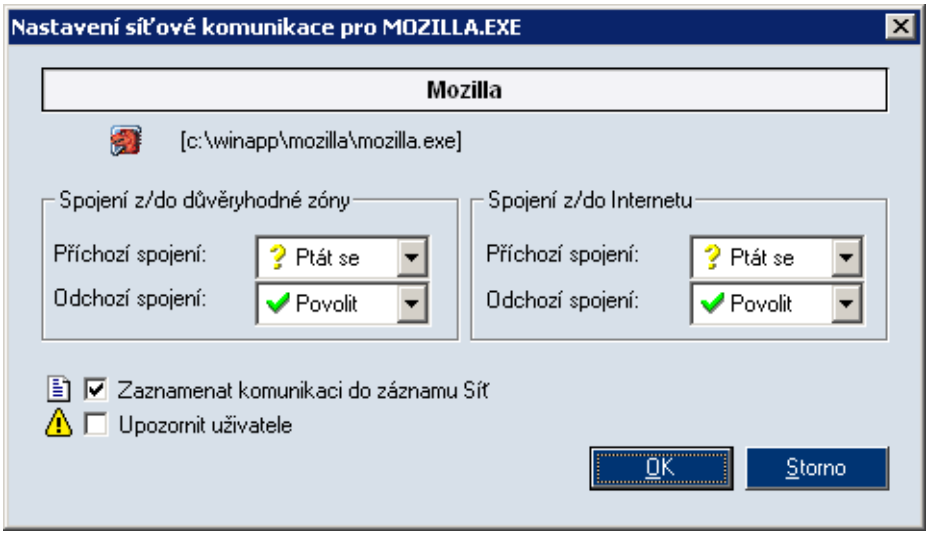
2. Kliknutím myší na akci (ve sloupci *Důvěryhodné* nebo *Internet*):
   - levým tlačítkem se akce cyklicky přepíná: *Povolit* — *Zakázat* — *Ptát se*
   - pravým tlačítkem se zobrazí kontextové menu, z něhož lze vybrat požadovanou akci.

Obrázek 7.5 Pravidla pro aplikace — volba akce

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.



Obrázek 7.6 Pravidla pro aplikace — dialog pro definici pravidla

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 16.4).

Volba *Upozornit uživatele* zapíná zobrazování upozornění uživateli (viz kapitola 5.5) při zachycení komunikace vyhovující tomuto pravidlu.

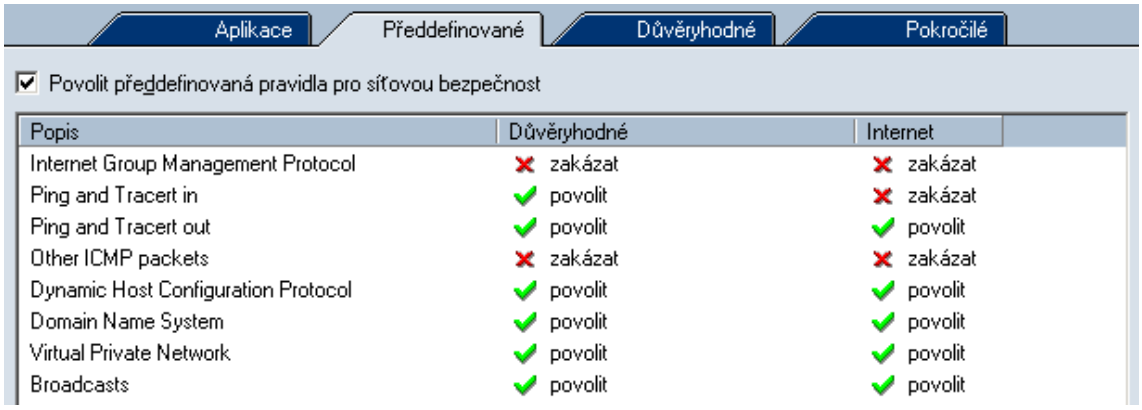
7.3 Předdefinovaná pravidla pro síťovou komunikaci

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 7.2 a 5.2).



Obrázek 7.7 Sekce *Síťová bezpečnost / Předdefinované* — předdefinovaná pravidla pro síťovou komunikaci

Volba *Povolit předdefinovaná pravidla pro síťovou bezpečnost* povoluje/zakazuje předdefinovaná pravidla pro síťovou komunikaci. Je-li tato volba vypnuta, pak jsou předdefinovaná pravidla ignorována a *Kerio Personal Firewall* pracuje pouze s pravidly pro aplikace (viz kapitola 7.2) a s rozšířeným paketovým filtrem (viz kapitola 8).

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* povoluje/zakazuje vytváření VPN protokolem *PPTP* (proprietární protokol firmy *Microsoft*).

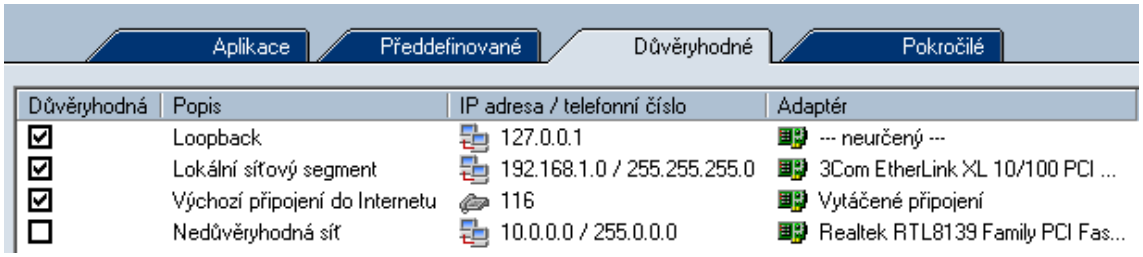
Broadcasts

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

7.4 Důvěryhodná zóna

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 *Důvěryhodné* v sekci *Síťová bezpečnost*.



Obrázek 7.8 Sekce *Síťová bezpečnost / Důvěryhodné* — definice zóny

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).

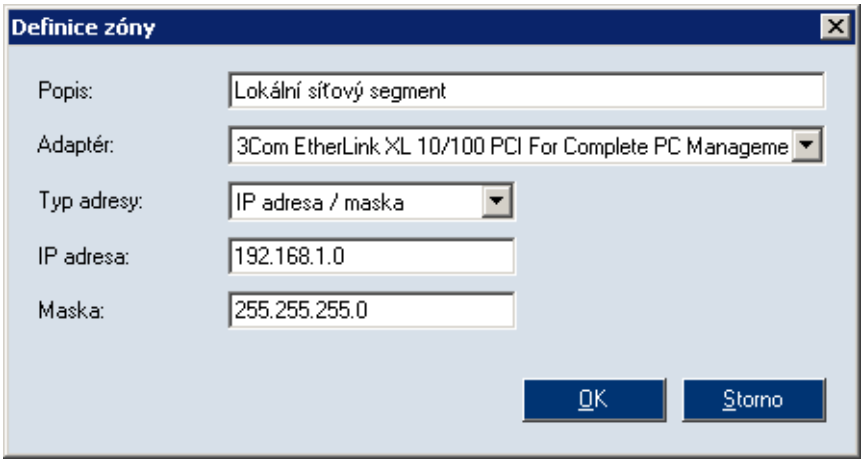
Důvěryhodná zóna vždy obsahuje jednu předdefinovanou položku *Loopback*, kterou nelze změnit ani odstranit. Jedná se o lokální zpětnovazební adresu (loopback) — tato adresa je vždy považována za důvěryhodnou.

Zaškrtávací pole ve sloupci *Důvěryhodná* znamená, že tato položka (síť, rozsah adres atd.) patří do důvěryhodné zóny. Položky, u nichž není toto pole zaškrtnuto, explicitně specifikují IP adresy, které nejsou považovány za důvěryhodné. Takto lze mj. specifikovat výjimky (např. nedůvěryhodný počítač v důvěryhodné síti).

Položky v záložce *Důvěryhodné* zároveň určují síťová rozhraní (tj. síťové adaptéry, vytáčená připojení, VPN připojení atd.), které *Kerio Personal Firewall* zná. Pokud firewall detekuje síťové rozhraní, které se nevyskytuje v žádné položce důvěryhodné zóny, pak se dotáže uživatele, zda je toto rozhraní připojené do důvěryhodné sítě či nikoliv, a automaticky vytvoří odpovídající položku (podrobnosti viz kapitola 2.2).

Definice položek důvěryhodné zóny

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).



Obrázek 7.9 Definice položky důvěryhodné zóny

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

Poznámky:

1. 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).

2. Je-li v položce *Adaptér* vybrána vytáčená linka, pak dialog *Definice zóny* umožňuje nastavit chování firewallu při změně telefonního čísla. Podrobnosti naleznete v kapitole 7.8.

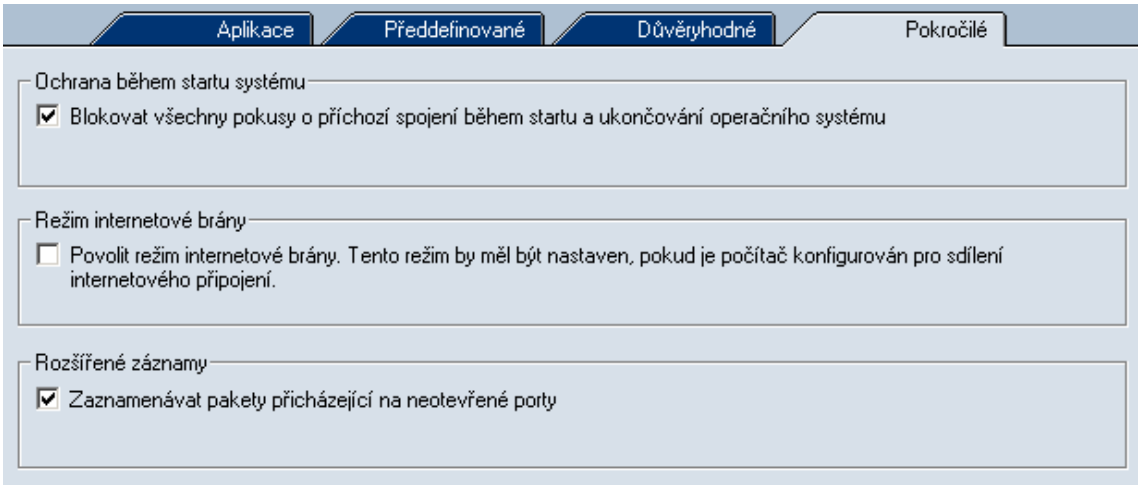
7.5 Pokročilá nastavení síťové bezpečnosti

Záložka *Pokročilé* v sekci *Síťová bezpečnost* obsahuje volby pro upřesňující nastavení zabezpečení a pro sledování nežádoucí komunikace.

Ochrana během startu systému

Volba *Blokovat všechny pokusy o příchozí spojení...* zapíná/vypíná nízkoúrovňovou ochranu počítače (podrobnosti viz kapitola 7.6).

Ve výchozí konfiguraci *Kerio Personal Firewallu* je nízkoúrovňová ochrana zapnuta. Její vypnutí může být užitečné při testování a řešení problémů (např. při potížích se vzdálenou správou počítače, který *Kerio Personal Firewall* chrání).



Obrázek 7.10 Sekce *Síťová bezpečnost / Pokročilé*

Z bezpečnostních důvodů doporučujeme nevypínat nízkoúrovňovou ochranu, pokud to není nezbytně nutné.

Režim internetové brány

Volba *Povolit režim internetové brány* přepíná firewall do speciálního režimu pro ochranu 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!

Upozornění: Kerio Personal Firewall v režimu internetové brány povoluje komunikaci mezi lokální sítí a Internetem, stále však chrání pouze počítač, na kterém je nainstalován! Nasazením produktu *Kerio Personal Firewall* na internetovou bránu nevznikne plnohodnotný síťový firewall!

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).

Rozšířené záznamy

Volba *Zaznamenávat pakety přicházející na neotevřené porty* aktivuje záznam zachycených paketů s cílovými porty, které nepatří žádnému procesu v lokálním operačním systému. Tyto pakety jsou automaticky zahazovány, mohou však signalizovat pokus o útok (scannování portů).

Poznámka: Režim internetové brány a záznam paketů na neotevřené porty nelze vzájemně kombinovat. V režimu internetové brány musí firewall všechny takové pakety propouštět (jsou určeny jiným počítačům).

7.6 Ochrana počítače nízkoúrovňovým ovladačem firewallu

Nízkoúrovňový ovladač pro síťovou komunikaci *Kerio Personal Firewallu* chrání počítač i v době, kdy je firewall vypnutý. Tato situace nastává typicky při startu systému (doba od aktivace síťových připojení do chvíle, kdy se služba automaticky spustí) a při aktualizaci produktu (při instalaci nové verze *Kerio Personal Firewallu* je služba automaticky zastavena a znovu spuštěna až po restartu serveru), případně pokud se služba *Personal Firewall Engine* (viz kapitola 4.1) po startu systému z nějakého důvodu nespustí.

Ve výchozí instalaci *Kerio Personal Firewall* je nízkoúrovňová ochrana zapnuta. V případě potřeby je možno ji kdykoliv vypnout a opět zapnout v uživatelském rozhraní firewallu (sekce *Síťová bezpečnost*, záložka *Pokročilé* — viz kapitola 7.5).

Je-li nízkoúrovňová ochrana zapnuta, pak se nízkoúrovňový ovladač pro síťovou komunikaci *Kerio Personal Firewallu* chová následovně:

- Po startu operačního systému povoluje pouze odchozí komunikaci a blokuje veškerou příchozí komunikaci. Server je tak stále chráněn, jeho služby jsou však nedostupné.

  Pokud se do 5 minut od startu systému nespustí *Personal Firewall Engine*, přejde ovladač do stavu, kdy povoluje veškerou komunikaci. Tím je zajištěno, že komunikace se serverem nebude blokována v případech, kdy se z nějakého důvodu nepodaří *Personal Firewall Engine* spustit.

- Po spuštění *Personal Firewall Engine* firewall povoluje a blokuje komunikaci podle nastavených pravidel síťové bezpečnosti.

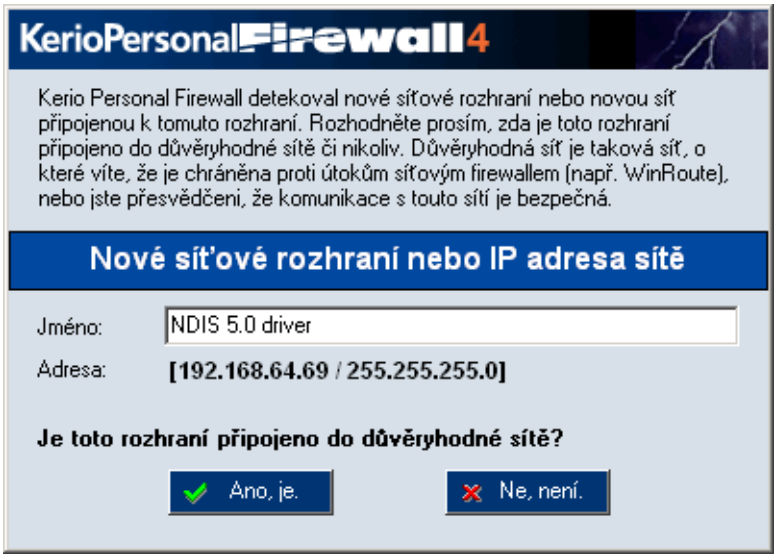
- Při vypínání (restartu) operačního systému ovladač firewallu zablokuje veškerou příchozí i odchozí komunikaci. Tak je server chráněn po dobu, kdy je služba *Personal Firewall Engine* již zastavena, ale síťový subsystém je dosud aktivní.

- Při ukončení služby *Kerio Personal Firewall* přejde ovladač do režimu, kdy povoluje veškerou síťovou komunikaci. Tento stav nastává pouze při ručním ukončení firewallu nebo po pádu *Personal Firewall Engine*.

7.7 Detekce nových síťových rozhraní

Je-li při instalaci zvolen výchozí režim *Advanced* (viz kapitolu 2.2), pak *Kerio Personal Firewall* automaticky detekuje aktivní síťová rozhraní počítače, na kterém je nainstalován. Pro každé nově detekované rozhraní zobrazí dotaz, zda je toto rozhraní připojeno do důvěryhodné sítě či nikoliv.

Poznámka: 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 kapitolu 7.4).



Obrázek 7.11 Detekce nového (dosud neznámého) síťového rozhraní

V poli *Jméno* je uveden název příslušného síťového adaptéru, v položce *Adresa* jeho IP adresa a maska subsítě, do které je připojen. Jméno rozhraní lze v tomto dialogu upravit (pro lepší přehlednost jej doporučujeme nahradit srozumitelným popisem, např. *Síťová karta*, *Linka do Internetu* apod.). Standardně je jako jméno rozhraní použit identifikační řetězec adaptéru načtený z příslušného ovladače zařízení.

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 změnit (detailní informace naleznete v kapitole 7.4).

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 navíc zobrazí informace o telefonním čísle, které je vytáčeno. Uživatel může připojení na toto telefonní číslo povolit nebo zakázat.

   Kerio Personal Firewall dokáže detekovat, zda nedošlo ke změně telefonního čísla od posledního vytočení linky (ochrana proti nežádoucí změně nastavení telefonického připojení). Podrobnosti naleznete v kapitole 7.8.

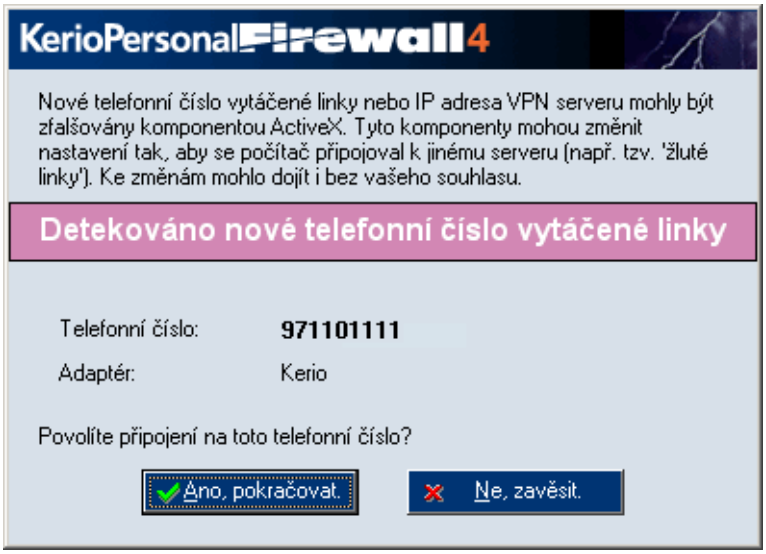
7.8 Kontrola vytáčených telefonních čísel

Kerio Personal Firewall dokáže detekovat a blokovat změny telefonních čísel vytáčených linek. Toto je ochrana proti nežádoucímu přesměrování telefonického připojení ke službě s vysokým tarifem. Takové přesměrování může provést např. ActiveX objekt na WWW stránce, a to zcela bez vědomí uživatele. V případě změny telefonního čísla se *Kerio Personal Firewall* nejprve dotáže uživatele, zda se změnou telefonního čísla souhlasí. Pokud ne, ihned linku zavěsí. Uživatel je tak chráněn před placením vysokých částek za připojení k nežádoucím službám.

Jak kontrola vytáčených čísel funguje?

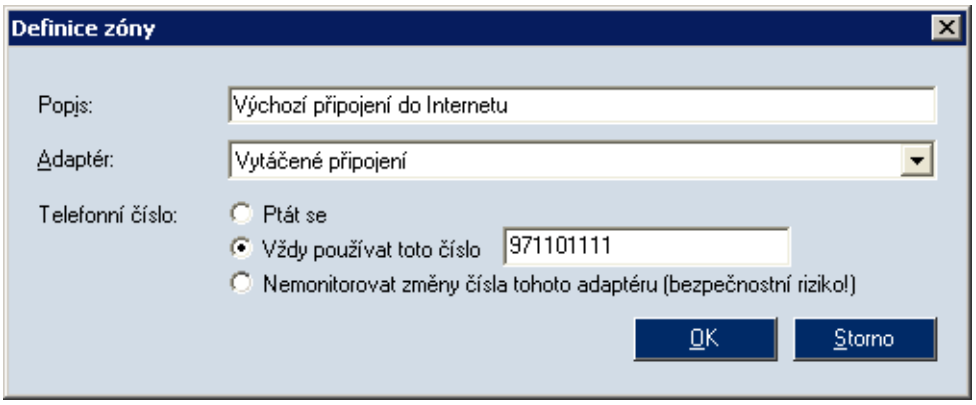
Při prvním vytočení telefonického připojení, které firewall dosud nezná, se zobrazí dotaz, zda je toto rozhraní připojeno do důvěryhodné sítě (stejně jako při detekci nového síťového adaptéru — viz kapitola 7.4). Vytáčené připojení bude zobrazováno jako rozhraní v sekci *Síťová bezpečnost / Důvěryhodná zóna*.

Po dotazu na zařazení adaptéru do důvěryhodné zóny je zobrazen dialog s informací o novém telefonním čísle.



Obrázek 7.12 Detekce nového čísla vytáčené linky

V dialogu pro změnu příslušné položky důvěryhodné zóny (po stisknutí tlačítka *Změnit*) lze nastavit chování firewallu při změně telefonního čísla vytáčeného připojení.



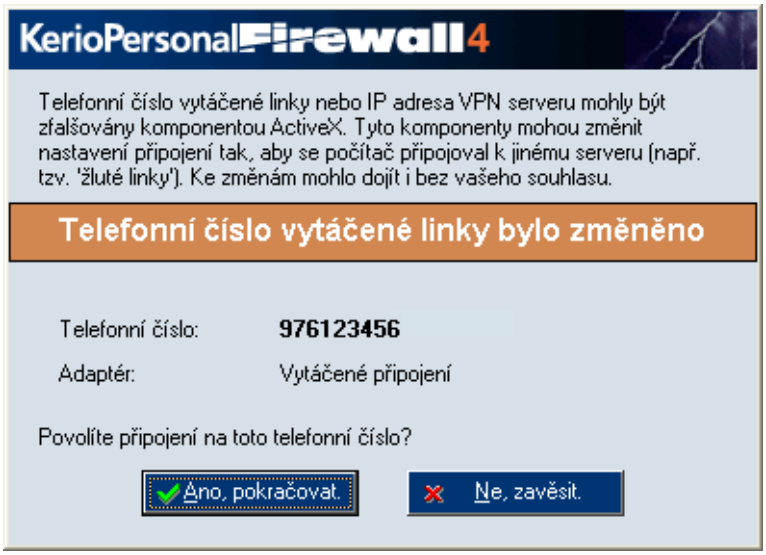
Obrázek 7.13 Nastavení kontroly telefonního čísla vytáčené linky

Volba *Telefonní číslo* nabízí následující možnosti:

- *Ptát se — Kerio Personal Firewall* se při vytočení linky dotáže uživatele, zda akceptuje příslušné telefonní číslo. V případě, že ano, pak si toto číslo zapamatuje. V opačném případě linku ihned zavěsí.

  Akceptuje-li uživatel nové telefonní číslo, pak dojde k automatickému přepnutí na volbu *Vždy používat toto číslo* a příslušné číslo se uloží.

- *Vždy používat toto číslo* — firewall předpokládá, že telefonní číslo linky se nebude měnit. Při detekci jakékoliv změny telefonního čísla ze zobrazí dialog s informací o novém čísle a dotazem, zda uživatel změnu čísla akceptuje.



Obrázek 7.14 Detekce změny čísla vytáčené linky

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, povolí vytočení linky a zapamatuje si nové číslo. Tlačítko *Ne, zavěsit* znamená zamítnutí změny — linka bude zavěšena.

- *Nesledovat změny čísla na tomto rozhraní* — firewall bude ignorovat změny telefonního čísla a vždy povolí vytočení linky. Tuto volbu lze využít např. pro testovací účely, kdy se bude telefonní číslo často měnit.

  Upozornění: Tato volba představuje bezpečnostní riziko (firewall nedetekuje případnou nežádoucí změnu telefonního čísla) a nedoporučujeme ji proto nastavovat na výchozím internetovém připojení!

Kapitola 8

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:

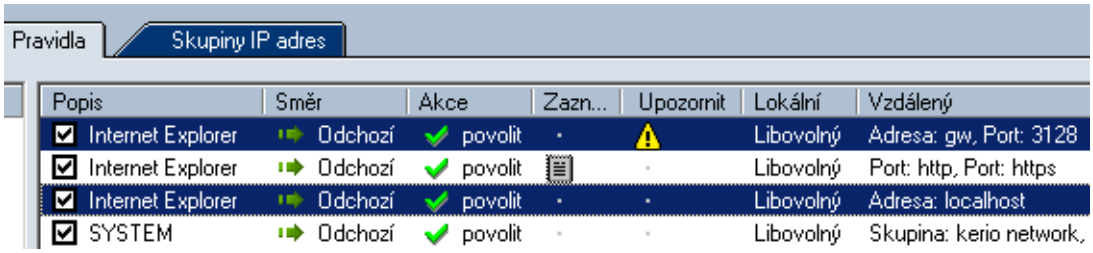
- Ručně — stisknutím tlačítka *Paketový filtr...* v sekci *Síťová bezpečnost*, záložka *Aplikace* se otevře okno *Rozšířený paketový filtr*, ve kterém lze prohlížet, upravovat a rušit pravidla paketového filtru (podrobnosti viz dále).
- Automaticky, resp. poloautomaticky — při zachycení komunikace, pro kterou nebylo nalezeno odpovídající pravidlo, je zobrazen dialog *Upozornění na spojení* (viz kapitola 5.2); 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.).

8.1 Pravidla paketového filtru

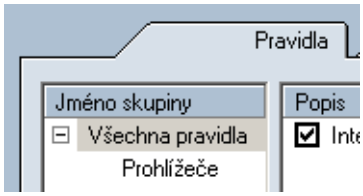
Pravidla rozšířeného paketového filtru se zobrazují v záložce *Pravidla* okna *Rozšířený paketový filtr*.

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 nebo klávesami *Ctrl + šipka nahoru*, *Ctrl + šipka dolů* lze pořadí pravidel v seznamu upravit dle potřeby. Díky těmto vlastnostem je možno vytvářet složitější kombinace filtrovacích pravidel.



Obrázek 8.1 Pravidla paketového filtru

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*.



Obrázek 8.2 Skupiny pravidel paketového filtru

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 (dialog pro úpravu pravidla lze také otevřít dvojitým kliknutím myší na vybrané pravidlo)
- *Přidat* — přidání nového pravidla na konec seznamu
- *Vložit* — přidání (vložení) nového pravidla na aktuální pozici (nad označené pravidlo)
- *Odebrat* — smazání označeného pravidla

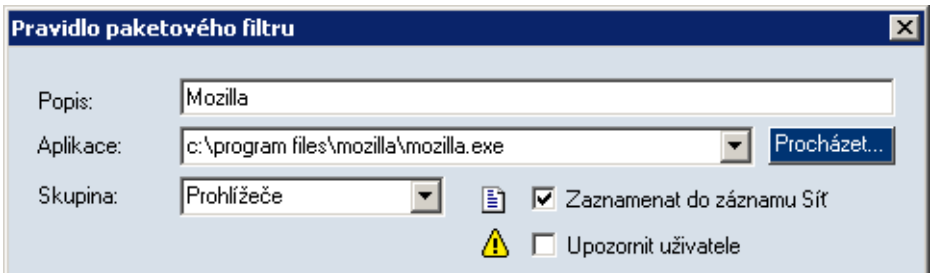
Poznámky:

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

2. Přidržením klávesy *Ctrl* nebo *Shift* lze označit více pravidel současně. Takto označenou skupinu pravidel lze pouze přesunout nebo smazat. Tlačítko *Změnit* v tomto případě otevře dialog pro změnu prvního (horního) označeného pravidla. Funkce *Vložit* vloží nové pravidlo nad první pravidlo skupiny.

Vytvoření nebo změna pravidla

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



Obrázek 8.3 Pravidlo paketového filtru

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 5.2).

Zaznamenat do záznamu Síť

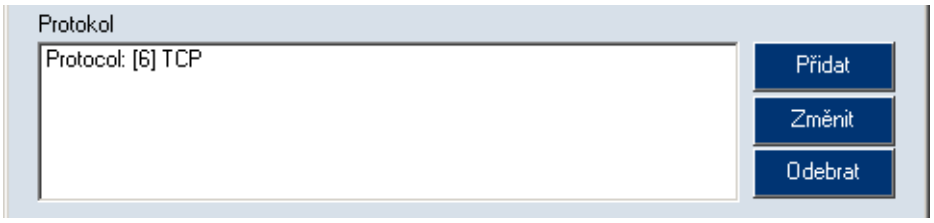
Zapnutí/vypnutí záznamu komunikace vyhovující tomuto pravidlu do záznamu *Síť* (viz kapitola 16.4).

Upozornit uživatele

Zapnutí/vypnutí zobrazení upozornění uživateli (viz kapitola 5.5) 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).

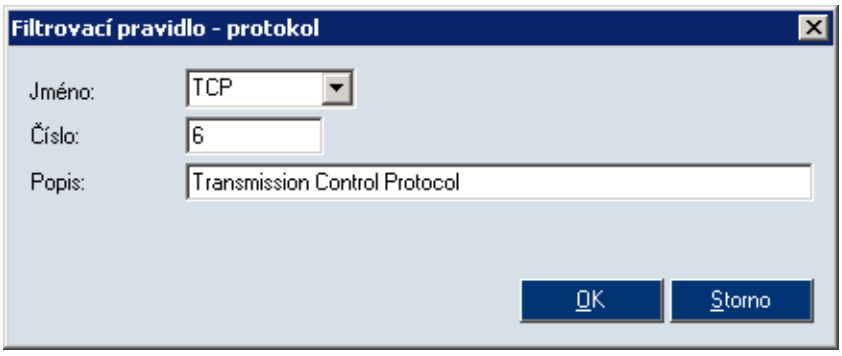


Obrázek 8.4 Pravidlo paketového filtru — protokoly

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.

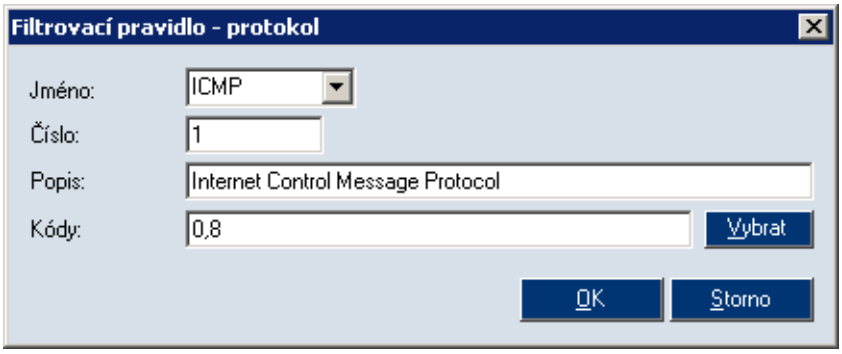


Obrázek 8.5 Pravidlo paketového filtru — přidání protokolu

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.

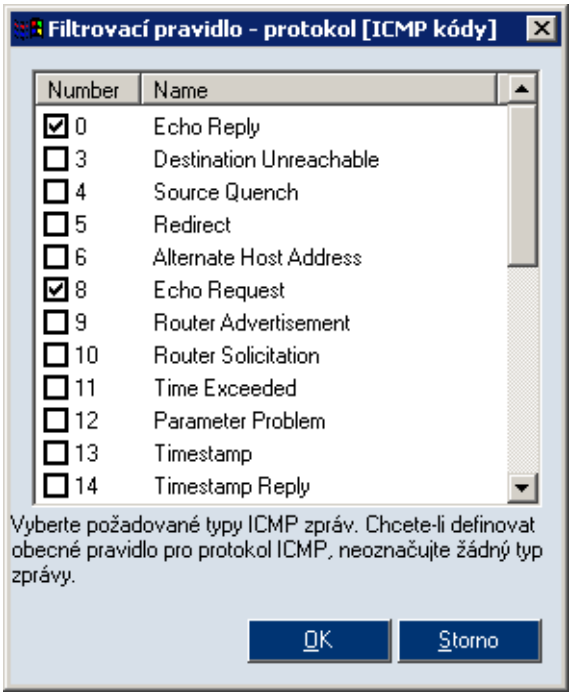
Při výběru protokolu ICMP se v dialogu zobrazí speciální položka *Kódy*. V ní lze nastavit typy ICMP zpráv, pro které bude pravidlo platit.



Obrázek 8.6 Pravidlo paketového filtru — protokol ICMP

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*.



Obrázek 8.7 Pravidlo paketového filtru — výběr typů ICMP zpráv

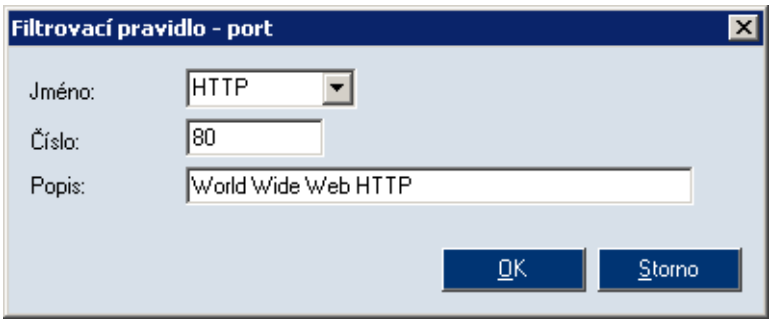
Lokální

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.

Obrázek 8.8 Pravidlo paketového filtru — port (síťová služba)

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).



Obrázek 8.9 Pravidlo paketového filtru — přidání portu (síťové služby)

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

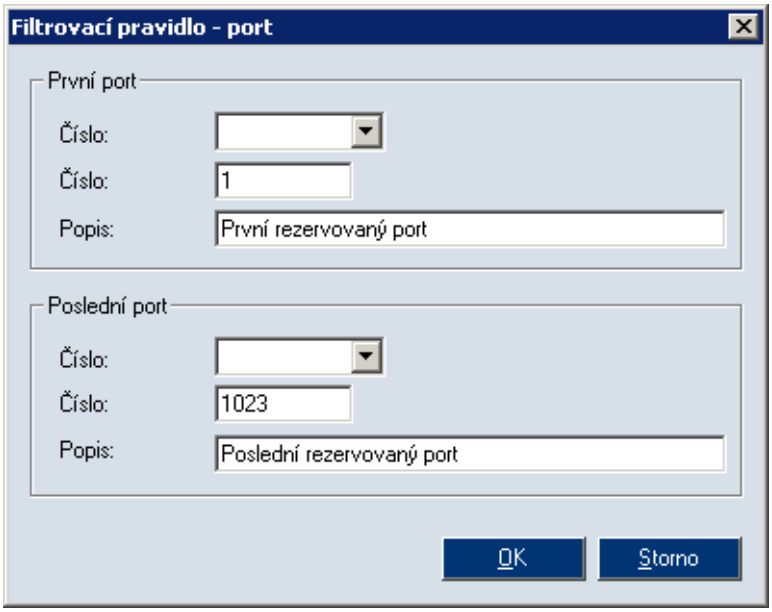
Vzdálený

Specifikace vzdálené strany spojení. Dle potřeby je možno zadat IP adresy (počítače) nebo porty (služby), případně obojí. Pravidlo se pak uplatní, jestliže zachycený paket bude obsahovat některou z IP adres a zároveň některý z portů uvedených v poli *Vzdálený*.

Vzdálené porty mohou být opět zadány jednotlivě (*Přidat port*) nebo jako rozsah portů (*Přidat rozsah portů*) — viz výše.

Vzdálené počítače mohou být specifikovány jako:

- jedna IP adresa (*Přidat adresu*)

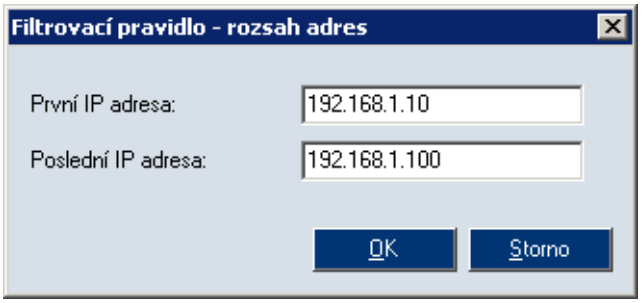


Obrázek 8.10 Pravidlo paketového filtru — přidání rozsahu portů

Obrázek 8.11 Pravidlo paketového filtru — vzdálená IP adresa (počítač) a port (služba)

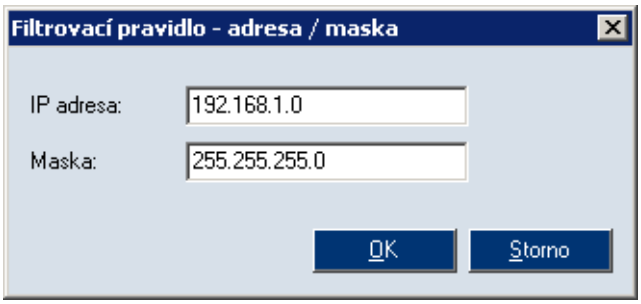
Obrázek 8.12 Pravidlo paketového filtru — přidání IP adresy

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



Obrázek 8.13 Pravidlo paketového filtru — přidání IP rozsahu IP adres

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



Obrázek 8.14 Pravidlo paketového filtru — přidání susbsítě

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

Obrázek 8.15 Pravidlo paketového filtru — přidání skupiny IP adres

Jednotlivé možnosti zadání portů a IP adres lze libovolně kombinovat.

Obrázek 8.16 Pravidlo paketového filtru — nastavení směru komunikace a akce

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 rozšířený 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)

8.2 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*.

Obrázek 8.17 Paketový filtr — skupiny IP adres

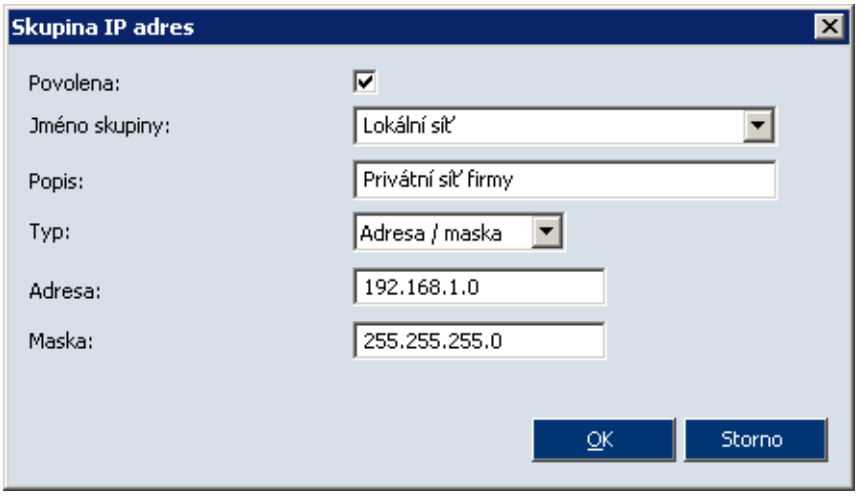
Okno obsahuje dva sloupce:

- *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.



Obrázek 8.18 Paketový filtr — přidání položky do skupiny IP adres nebo vytvoření nové skupiny

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 vnořovat).

Kapitola 9

Interní pravidla firewallu

Kerio Personal Firewall obsahuje předdefinovaná pravidla pro povolení síťové komunikace v určitých případech (např. registrace licence či aktualizace produktu) a povolení spuštění určitých aplikací (systémových komponent).

Interní pravidla firewallu mají přednost před uživatelsky definovanými pravidly. Uživatel nemůže interní pravidla vypnout ani změnit.

9.1 Interní pravidla pro síťovou komunikaci

Tato pravidla zajišťují povolení síťové komunikace mezi jednotlivými komponentami *Kerio Personal Firewallu* při lokální nebo vzdálené správě, připojení na servery firmy *Kerio Technologies* při registraci licence nebo kontrole nové verze apod.

Interní pravidla pro síťovou komunikaci jsou uživateli skryta — v *Personal Firewall GUI* se nezobrazují.

Vzdálená konfigurace

Toto pravidlo povoluje připojení *Personal Firewall GUI* k *Personal Firewall Engine*. Je-li povolena vzdálená správa (viz kapitola 6.3), pak je připojení povoleno z libovolného počítače, v opačném případě pouze z lokálního počítače.

Podmínka	Aplikace	Směr	Protokol	Vzd. port	Vzd. adresa
Vzd. správa povolena	`kpf4ss.exe`	příchozí	TCP+UDP	`44334`	libovolná
Vzd. správa zakázána	`kpf4ss.exe`	příchozí	TCP+UDP	`44334`	`localhost`

Komunikace Personal Firewall GUI s Personal Firewall Engine

Toto pravidlo povoluje *Personal Firewall GUI* navázat spojení na *Personal Firewall Engine* (připojení k lokální správě).

Poznámka: Toto pravidlo povoluje pouze lokální připojení (tj. připojení k *Personal Firewall Engine* na tomtéž počítači). V případě vzdálené správy je *Personal Firewall GUI* považováno za standardní síťovou aplikaci a použijí se pravidla pro síťovou komunikaci (viz kapitola 7).

Podmínka	Aplikace	Směr	Protokol	Vzd. port	Vzd. adresa
Platí vždy	`kpf4gui.exe`	odchozí	TCP+UDP	`44334`	`localhost`

Komunikace Personal Firewall Engine s Personal Firewall GUI

Pravidlo povoluje *Personal Firewall Engine* navázání spojení na *Personal Firewall GUI* (zobrazování dialogových oken, upozornění atd.).

Podmínka	Aplikace	Směr	Protokol	Vzd. port	Vzd. adresa
Vzd. správa povolena	`kpf4ss.exe`	odchozí	TCP+UDP	libovolný	libovolná
Vzd. správa zakázána	`kpf4ss.exe`	odchozí	TCP+UDP	libovolný	`localhost`

DNS dotazy

Pravidlo povoluje komponentám *Kerio Personal Firewallu* vysílat DNS dotazy na libovolný DNS server. DNS dotazy slouží např. ke zjišťování jmen počítačů pro zobrazování v *Personal Firewall GUI*, pro zjištění IP adresy cílového počítače při připojování ke vzdálené správě apod.

Podmínka	Aplikace	Směr	Protokol	Vzd. port	Vzd. adresa
Platí vždy	`kpf4ss.exe`	oba	UDP	`53`	libovolná
Platí vždy	`kpf4gui.exe`	oba	UDP	`53`	libovolná

Odesílání výpisů paměti

Je-li povoleno odesílání výpisu paměti v případě pádu aplikace do firmy *Kerio Technologies* (viz kapitola 6.3), pak toto pravidlo povoluje přístup na příslušný server.

Podmínka	Aplikace	Směr	Protokol	Vzd. port	Vzd. adresa
Odes. povoleno	`assist.exe`	odchozí	TCP	libovolný	`crashes.kerio.com`

Záznam blokovaných pop-up a pop-under oken

Je-li zapnuto blokování pop-up oken (viz kapitola 14.1), pak je na filtrované stránky dosazován speciální skript, který zasílá *Personal Firewall Engine* informace o blokovaných oknech. Komunikace probíhá protokolem TCP na speciálním portu (`44501`).

Podmínka	Aplikace	Směr	Protokol	Vzd. port	Vzd. adresa
Platí vždy	libovolná	odchozí	TCP	`44501`	`localhost`

Kontrola nových verzí

Toto pravidlo povoluje přístup na server pro zjišťování a stahování nových verzí programu *Kerio Personal Firewall*.

Poznámka: K tomuto účelu může být využito více různých serverů, proto není server v pravidle specifikován.

Podmínka	Aplikace	Směr	Protokol	Vzd. port	Vzd. adresa
Proxy server	`kpf4ss.exe`	odchozí	TCP	`proxy_port*`	`proxy_ip*`
Přímý přístup	`kpf4ss.exe`	odchozí	TCP	libovolný	libovolná

*) IP adresu a port proxy serveru zjišťuje *Kerio Personal Firewall* automaticky z nastavení operačního systému (*Možnosti sítě Internet* v *Ovládacích panelech*).

Registrace produktu

Toto pravidlo umožňuje registraci licence programu *Kerio Personal Firewall* (viz kapitola 3.2) na příslušném serveru.

Podmínka	Aplikace	Směr	Protokol	Vzd. port	Vzd. adresa
Proxy server	`kpf4ss.exe`	odchozí	TCP	`prx_port*`	`prx_ip*`
Přímý přístup	`kpf4ss.exe`	odchozí	TCP	`443`	`secure.kerio.com`

*) IP adresu a port proxy serveru zjišťuje *Kerio Personal Firewall* automaticky z nastavení operačního systému (*Možnosti sítě Internet* v *Ovládacích panelech*).

Záznam na Syslog server

Je-li povolen záznam na *Syslog* server (viz kapitola 16.3), pak toto pravidlo povoluje navázání spojení *Personal Firewall Engine* se *Syslog* serverem.

Podmínka	Aplikace	Směr	Protokol	Vzd. port	Vzd. adresa
Syslog povolen	`kpf4ss.exe`	odchozí	UDP	`sslg_port*`	`sslg_ip*`

*) IP adresa a port *Syslog* serveru specifikované v sekci *Záznamy*, záložka *Nastavení*.

9.2 Interní pravidla systémové bezpečnosti

Tato pravidla povolují spouštění součástí operačního systému, na kterém je *Kerio Personal Firewall* nainstalován. Interní pravidla systémové bezpečnosti se zobrazují v sekci *Bezpečnost systému / Aplikace* (viz kapitola 13.2). Uživatel může v těchto pravidlech nastavovat akce, případně záznam událostí nebo zobrazování upozornění, nemůže však tato pravidla odstranit.

Některá z těchto interních pravidel se uplatňují pouze v určitých verzích operačního systému Windows (některé systémové komponenty se v jednotlivých verzích liší).

Pravidla pro součásti operačního systému

V následujícím popisu pravidel pro systémové komponenty jsou použity tyto symboly pro označení cesty k souboru:

- `WIN_DIR` — hlavní adresář operačního systému Windows (typicky `C:\WINNT` pro

Windows 2000, `C:\WINDOWS` pro Windows XP)

- `SYS_DIR` — systémový adresář Windows (typicky `C:\WINNT\SYSTEM32` pro Windows 2000 a `C:\WINDOWS\SYSTEM32` pro Windows XP)

1. Pravidla společná pro všechny podporované verze operačního systému Windows

Aplikace	Popis	Spuštění	Záměna	Spuštění jiné
`WIN_DIR\explorer.exe`	`Windows Explorer`	Povolit	Ptát se	Povolit

2. Pravidla specifická pro operační systémy Windows 2000/XP

Aplikace	Popis	Spuštění	Záměna	Spuštění jiné
`SYS_DIR\services.exe`	`Services app.`	Povolit	Ptát se	Povolit
`SYS_DIR\winlogon.exe`	`Logon app.`	Povolit	Ptát se	Povolit

3. Pravidla specifická pro operační systémy Windows 2000/XP

Aplikace	Popis	Spuštění	Záměna	Spuštění jiné
`SYS_DIR\svchost.exe`	`Generic Host Proc.`	Povolit	Ptát se	Povolit

4. Pravidla specifická pro operační systém Windows XP

Aplikace	Popis	Spuštění	Záměna	Spuštění jiné
`SYS_DIR\logonui.exe`	`Logon UI`	Povolit	Ptát se	Povolit
`SYS_DIR\csrss.exe`	`Client Server`	Povolit	Ptát se	Povolit
`SYS_DIR\smss.exe`	`Client Server`	Povolit	Ptát se	Povolit
`SYS_DIR\svchost.exe`	`Generic Host Proc.`	Povolit	Ptát se	Povolit

Pravidla pro komponenty Kerio Personal Firewallu

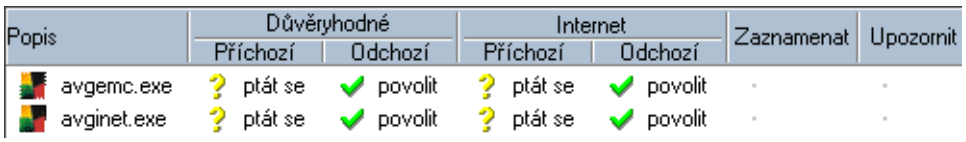
Tato pravidla povolují spouštění jednotlivých komponent aplikace *Kerio Personal Firewall* a pomocných programů. Uvedená pravidla jsou shodná pro všechny podporované verze operačního systému Windows.

Aplikace	Popis	Spuštění	Záměna	Spuštění jiné
KPF_DIR\kpf4gui.exe*	KPF GUI	Povolit	Povolit + záznam	Povolit
KPF_DIR\kpf4ss.exe*	KPF Service	Povolit	Povolit + zázn.	Povolit
KPF_DIR\assist.exe*	Core dumper	Povolit	Povolit + zázn.	Povolit
KPF_DIR\cfgconv.exe*	Conf. conv.	Povolit	Povolit + zázn.	Povolit

*) Výraz KPF_DIR znamená adresář, kde je *Kerio Personal Firewall* nainstalován (typicky C:\Program Files\Kerio\Personal Firewall 4).

9.3 Pravidla pro komponenty antivirového systému AVG

Je-li při prvním spuštění *Kerio Personal Firewallu* (tj. bezprostředně po instalaci, případně po smazání konfiguračního souboru kpf.cfg) v operačním systému detekován antivirus *AVG*, pak jsou do sekce *Síťová bezpečnost / Aplikace* (viz kapitola 7.2) automaticky přidána následující dvě pravidla povolující síťovou komunikaci komponent antiviru.



Obrázek 9.1 Síťová bezpečnost — pravidla pro komponenty antiviru AVG

- První pravidlo povoluje komunikaci komponenty *AVG E-mail Scanner* (*Kontrola pošty*) s poštovními servery (*E-mail Scanner* je zařazen mezi poštovního klienta a servery).
- Druhé pravidlo povoluje automatickou aktualizaci systému *AVG* a virové databáze z příslušných serverů.

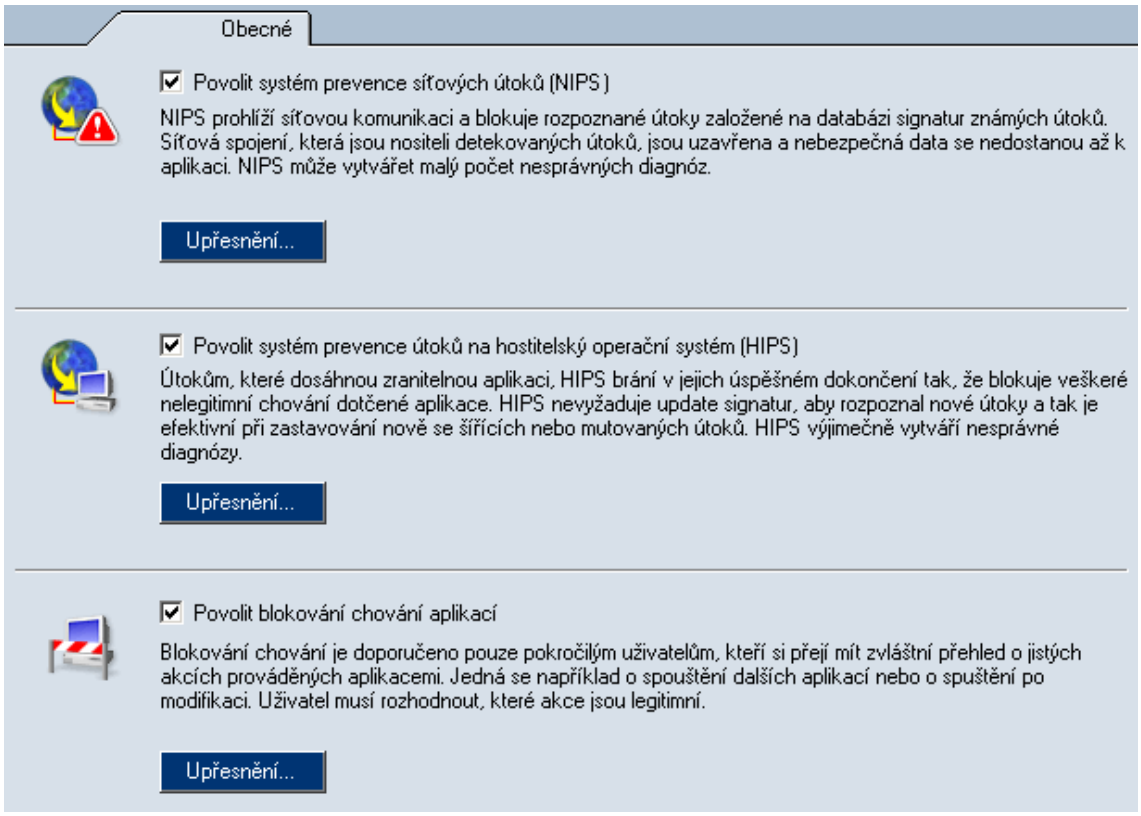
Pravidla pro antivirový systém *AVG* může uživatel libovolně měnit, případně odstranit. Budou-li tato pravidla odstraněna, bude *Kerio Personal Firewall* na komunikaci komponent *AVG* reagovat stejně jako na jinou neznámou komunikaci.

Upozornění: Používáte-li antivirus *AVG*, nedoporučujeme odstraňovat výše uvedená pravidla, pokud si nejste opravdu jisti, co děláte! Odstraněním těchto pravidel může dojít k zablokování aktualizace *AVG* (antivirus pak nebude schopen detekovat nové viry), případně k nefunkčnosti elektronické pošty.

Kapitola 10

Detekce útoků

Sekce *Útoky* v *Kerio Personal Firewallu* umožňuje nastavení ochrany proti různým typům útoků:



Obrázek 10.1 Sekce Útoky

- Detekce a prevence síťových útoků (NIPS) — tento systém rozpoznává a blokuje různé typy síťových útoků tak, že blokuje síťová spojení, která mohou přenášet nebezpečná data (více viz kapitolu 11).

- Detekce a prevence útoků na hostitelský operační systém (HIPS) — systém se zaměřuje na rozpoznávání a blokování technik, které útočníci nebo viry používají ke spuštění zákeřného kódu. HIPS je efektivní zejména při rozpoznávání nových nebo zmutovaných typů virů (kapitola 12).

- Blokování chování aplikací — systém umožňuje kontrolu chování aplikací, jako je například spouštění aplikace jinou aplikací nebo změna aplikace. Tato metoda je úspěšná zejména při rozpoznávání nových typů virů (více viz kapitolu 13).

Kapitola 11

Systém detekce a prevence síťových útoků (NIPS)

Kerio Personal Firewall dokáže rozpoznat a blokovat řadu známých typů síťových útoků. K tomuto účelu používá vlastní databázi útoků, která může být aktualizována s novými verzemi programu (z tohoto důvodu doporučujeme provádět aktualizaci *Kerio Personal Firewallu* vždy, když se automaticky nabídne).

Kerio Personal Firewall obsahuje systém detekce a prevence síťových útoků (*NIPS — Network Intrusion Prevention System*) kompatibilní s volně šiřitelným IDS *Snort* (`http://www.snort.org/`).

Poznámka: Pravidla systému detekce a prevence síťových útoků jsou uložena v podadresáři `config\IDSRules` instalačního adresáře

(typicky `C:\Program Files\Kerio\Personal Firewall 4\config\IDSRules`).

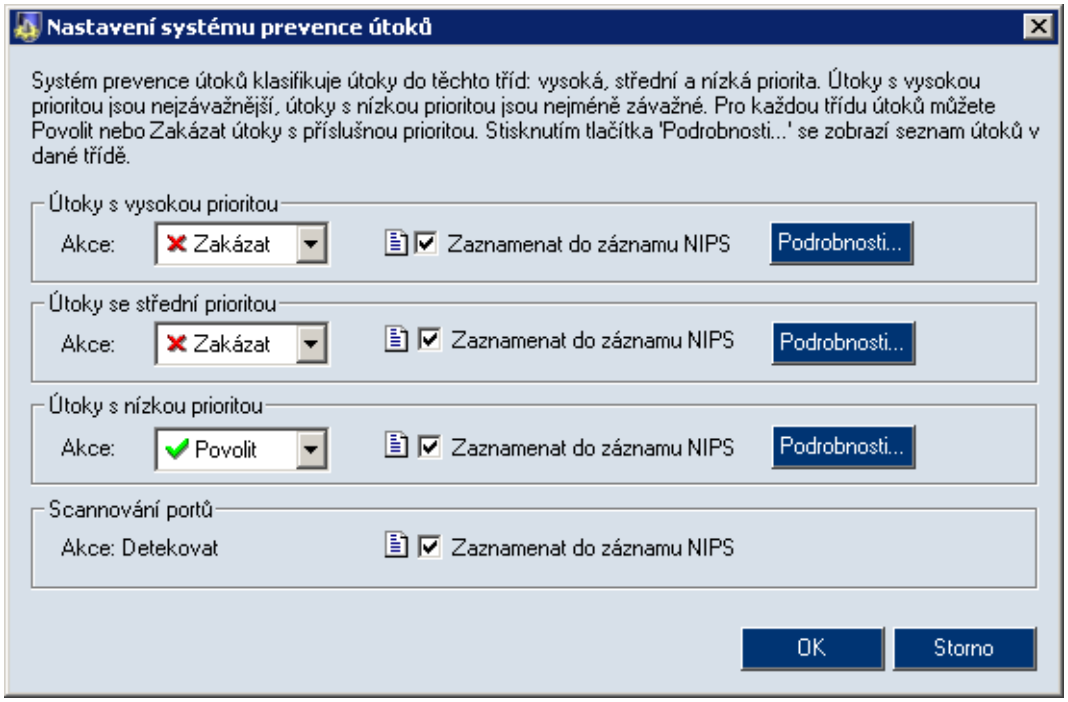
11.1 Nastavení systému detekce a prevence síťových útoků

Parametry systému detekce a prevence síťových útoků lze nastavit v sekci *Útoky* (obrázek 10.1).

Volba *Povolit systém detekce a prevence síťových útoků (NIPS)* 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



Obrázek 11.1 Sekce útoky — nastavení modulu detekce útoků

- *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.)

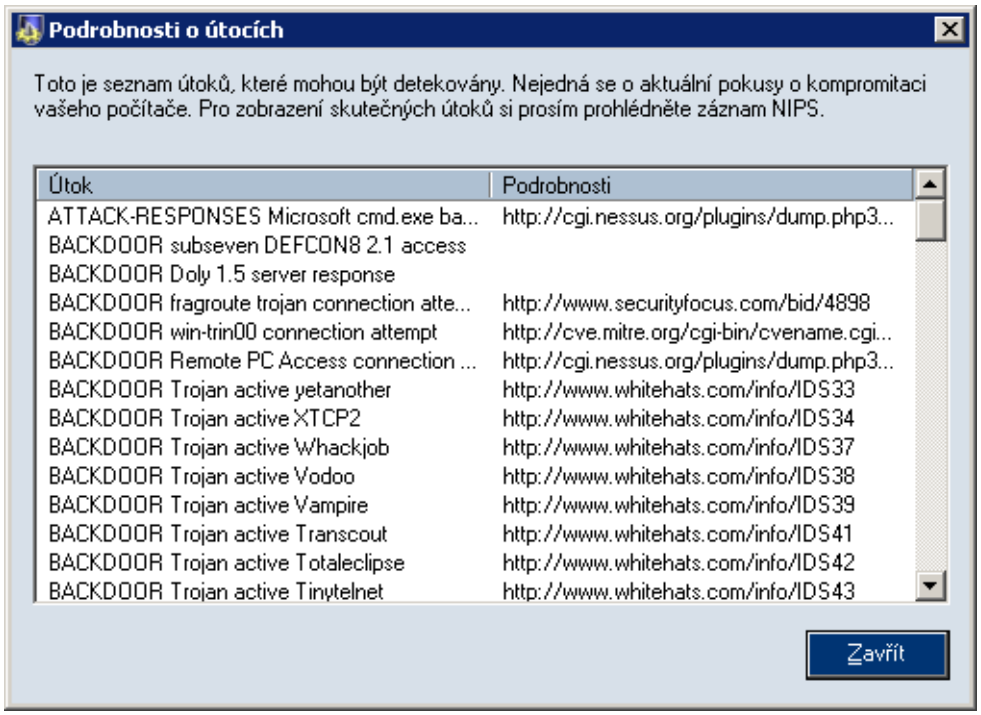
Pro každou z těchto skupin lze odděleně nastavit chování firewallu:

- *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 16.5).

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



Obrázek 11.2 Detekce útoků — podrobnosti o útocích, které *Kerio Personal Firewall* dokáže zachytit

Okno obsahuje název (popis) útoku (sloupec *Útok*) a třídu útoku (sloupec *Třída*). Podrobné informace naleznete na WWW stránkách systému detekce útoků *Snort* (`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 12

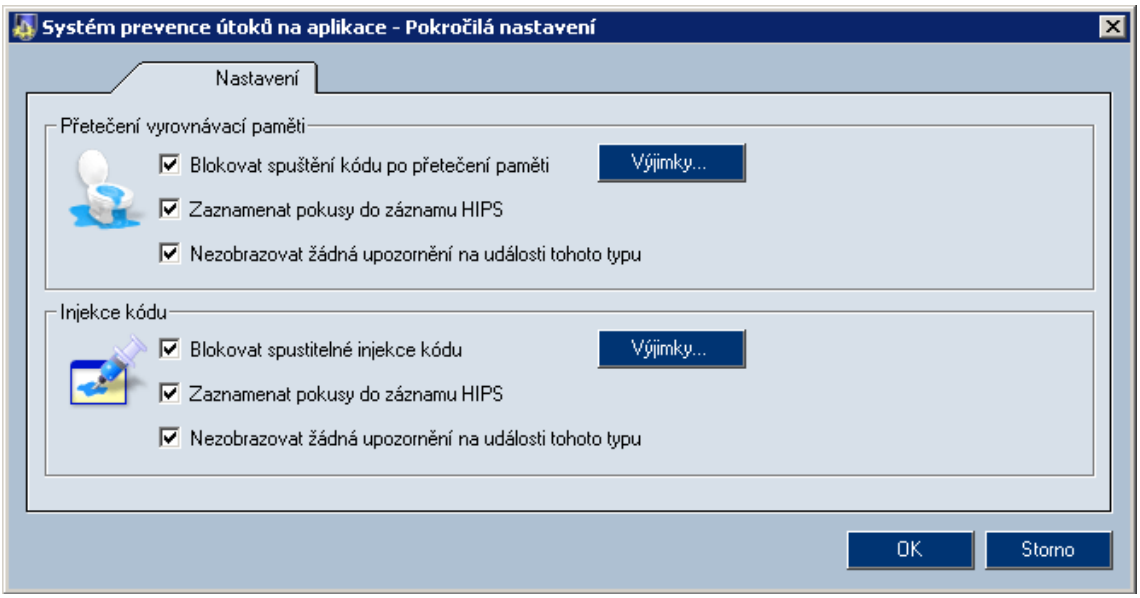
Systém detekce a prevence útoků na aplikace (HIPS)

HIPS (Host Intrusion and Prevention System) je zaměřen na detekci a blokování speciálních technik, které útočníci nebo viry používají ke spuštění zákeřného kódu. Legitimní aplikace za normálních okolností tyto techniky nepoužívají. Blokování těchto technik dokáže zabránit zneužití bezpečnostních chyb v aplikacích provozovaných na serveru. *HIPS* poskytuje ochranu i před novými bezpečnostními dírami, které běžné systémy detekce útoků nezachytí, protože je dosud nemají ve svých databázích.

12.1 Nastavení systému detekce útoků na aplikace

Parametry systému detekce útoků lze nastavit v sekci *Útoky* (obrázek 10.1).

HIPS dokáže detekovat a blokovat dvě nejrozšířenější techniky používané pro vykonání zákeřného kódu: *přetečení vyrovnávací paměti* (*Buffer Overflow*) a *Injekce kódu* (*Code Injection*) — zavedení spustitelného kódu do jiného procesu.



Obrázek 12.1 Sekce útoky — nastavení modulu prevence útoků

Přetečení vyrovnávací paměti

Technika *Přetečení vyrovnávací paměti* je založena na zneužití nedostatečné kontroly vstupních dat aplikace. Pokud není kontrolována velikost (délka) čtených dat, může útočník přepsat návratovou adresu spuštěného podprogramu a zajistit tak spuštění vlastního kódu. Tento kód je však spuštěn z oblasti paměti procesu vyhrazené pro data, což je nestandardní chování, které modul *HIPS* detekuje. Případné pokusy tohoto kódu o provedení potencionálně nebezpečných akcí (spuštění procesu, otevření souboru, navázání síťového spojení atd.) budou blokovány.

Blokovat spuštění kódu po přetečení paměti
: Volba umožňuje blokování spuštění kódu po přetečení vyrovnávací paměti.

Zaznamenat pokusy do záznamu HIPS
: Po zapnutí této volby se bude provádět záznam všech detekovaných útoků do logu *HIPS* (viz kapitolu 16.6).

Nezobrazovat žádná upozornění na události tohoto typu
: Po zaškrtnutí volby se nebudou při pokusu o útok zobrazovat upozorňující okna (kapitola 5.4).

Tlačítko *Výjimky* umožňuje zadat spustitelný soubor, na který se nebude kontrola na tento typ útoku vztahovat. Před zadáním každé výjimky důkladně zkontrolujte, zda se nejedná o útok.

Injekce kódu

Technika *Injekce kódu* je založena na zneužití oprávnění jiného spuštěného důvěryhodného procesu. Infikovaná aplikace (s příslušným oprávněním) zapíše zákeřný spustitelný kód do paměťového prostoru tohoto procesu nebo připojí dynamickou knihovnu k tomuto procesu. Pomocí speciálních volání operačního systému pak tento kód spustí. Takto útočník zajistí provedení svého kódu s oprávněním napadeného důvěryhodného procesu.

Modul *HIPS* detekuje a blokuje spouštění kódu zapsaného pomocí speciálních volání operačního systému do paměti důvěryhodného procesu. V tomto případě zpravidla nedochází ani k narušení správné funkce napadené aplikace.

Blokovat spustitelné injekce kódu
: Zaškrtnutím této volby bude zajištěno blokování útoku typu injekce kódu.

Zaznamenat pokusy do záznamu HIPS

Po zapnutí této volby se bude provádět záznam všech detekovaných útoků do logu *HIPS* (viz kapitolu 16.6).

Nezobrazovat žádná upozornění na události tohoto typu

Po zaškrtnutí volby se nebudou při pokusu o útok zobrazovat upozorňující okna (kapitola 5.4).

Techniku *Injekce kódu* mohou využívat i některé legitimní aplikace — tyto aplikace pak nebudou fungovat správně. V těchto případech umožňuje *Kerio Personal Firewall* definovat výjimky — seznam aplikací, kterým je povoleno používat tuto techniku. Výjimku na aplikaci lze definovat v dialogu *Výjimky injekce kódu* (tlačítko *Výjimky*), kde je možno vybrat příslušný spustitelný soubor.

Kapitola 13

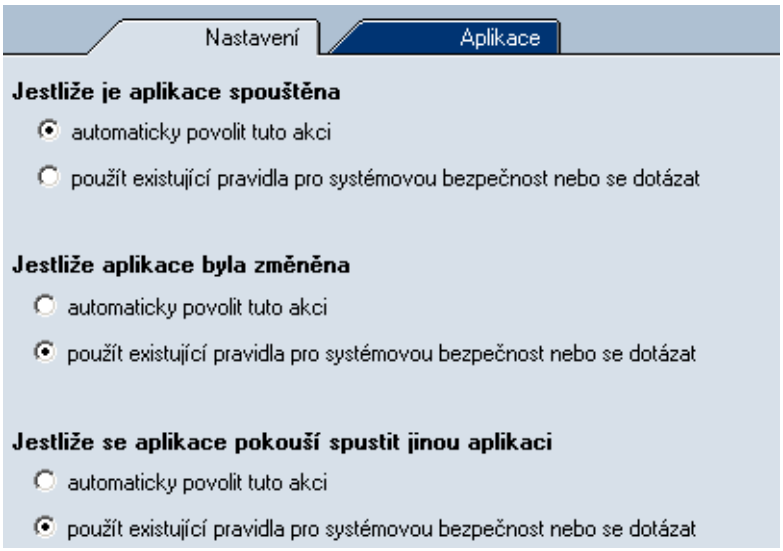
Blokování chování aplikací

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 nakažení 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 *Útoky* (obrázek 10.1).

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

13.1 Obecná pravidla



Obrázek 13.1 Blokování chování aplikací — obecná pravidla

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

- *Jestliže je aplikace spouštěna*

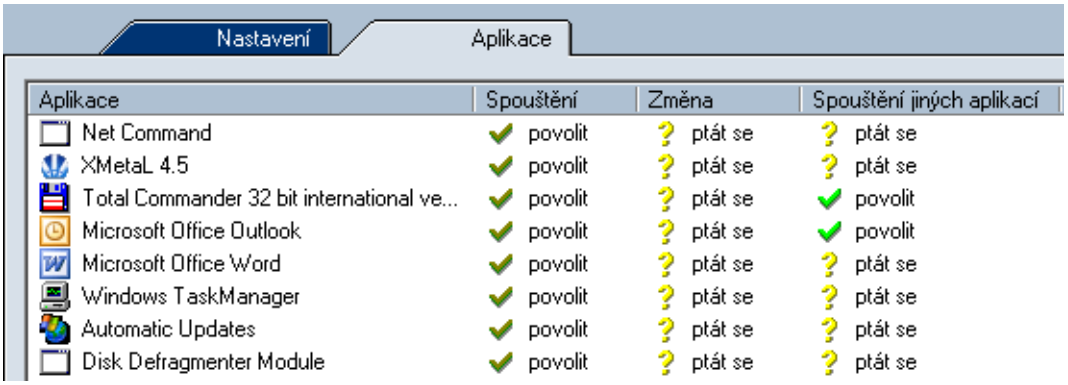
- *Jestliže aplikace byla změněna* — změna spustitelného souboru aplikace (při spuštění aplikace se vytvoří kontrolní součet spustitelného souboru a porovná se s kontrolním součtem, který má *Kerio Personal Firewall* uložen ve své databázi)
- *Jestliže se aplikace pokouší spustit jinou aplikaci*

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* použije pravidlo pro danou aplikaci (pokud existuje) nebo se dotáže uživatele, zda tuto akci povolí či nikoliv (viz kapitola 5.3)

13.2 Pravidla pro aplikace

Záložka *Aplikace* v sekci *Útoky* (*Blokování chování aplikací*) obsahuje pravidla pro spouštění a záměnu konkrétních aplikací.



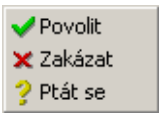
Obrázek 13.2 Blokování chování aplikací — pravidla pro aplikace

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:

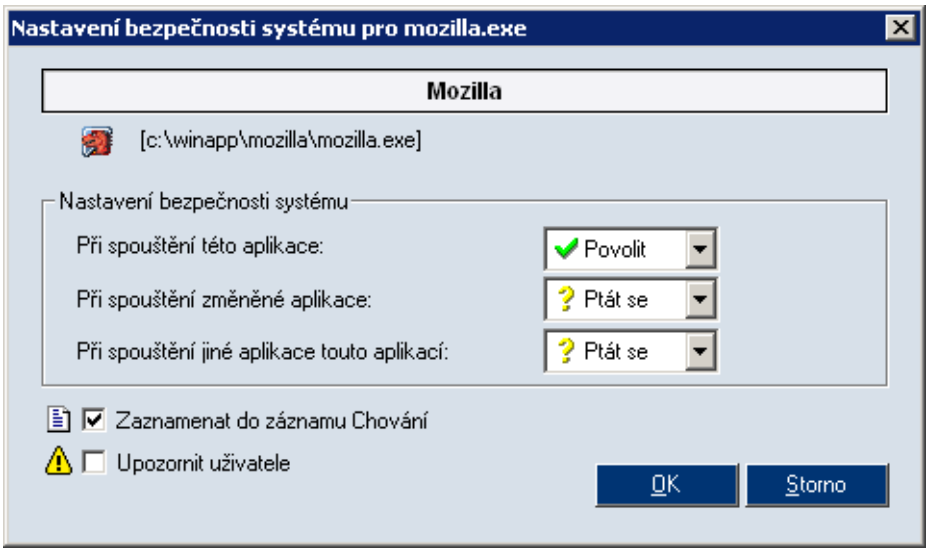
1. přímo v seznamu aplikací — klikáním levým tlačítkem na vybranou akci se cyklicky přepíná: *povolit*, *zakázat* a *ptát se* (dotázat se uživatele)

2. v kontextovém menu, které se zobrazí po kliknutí pravým tlačítkem na vybranou akci



Obrázek 13.3 Blokování chování aplikací — pravidla pro aplikace — výběr akce

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



Obrázek 13.4 Blokování chování aplikací — úprava pravidla pro aplikaci

- 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 Chování* 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 kapitolu 5.5) při aktivitě příslušné aplikace.

Kapitola 14

Filtrování obsahu WWW stránek

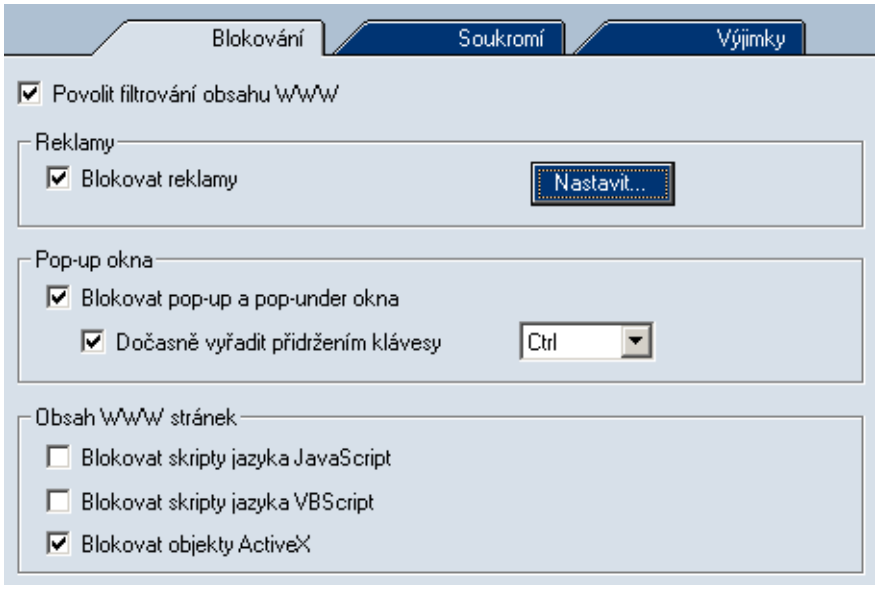
Filtr obsahu WWW stránek v *Kerio Personal Firewallu* má dvě hlavní funkce:

- 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.

14.1 Blokování reklam, skriptů a pop-up oken



Obrázek 14.1 Sekce *WWW / Blokování* — filtrování nežádoucích prvků WWW stránek

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).

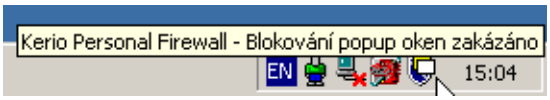
Blokovat pop-up a pop-under okna

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.



Obrázek 14.2 Ikona na nástrojové liště — indikace dočasného vypnutí blokování pop-up oken

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*).

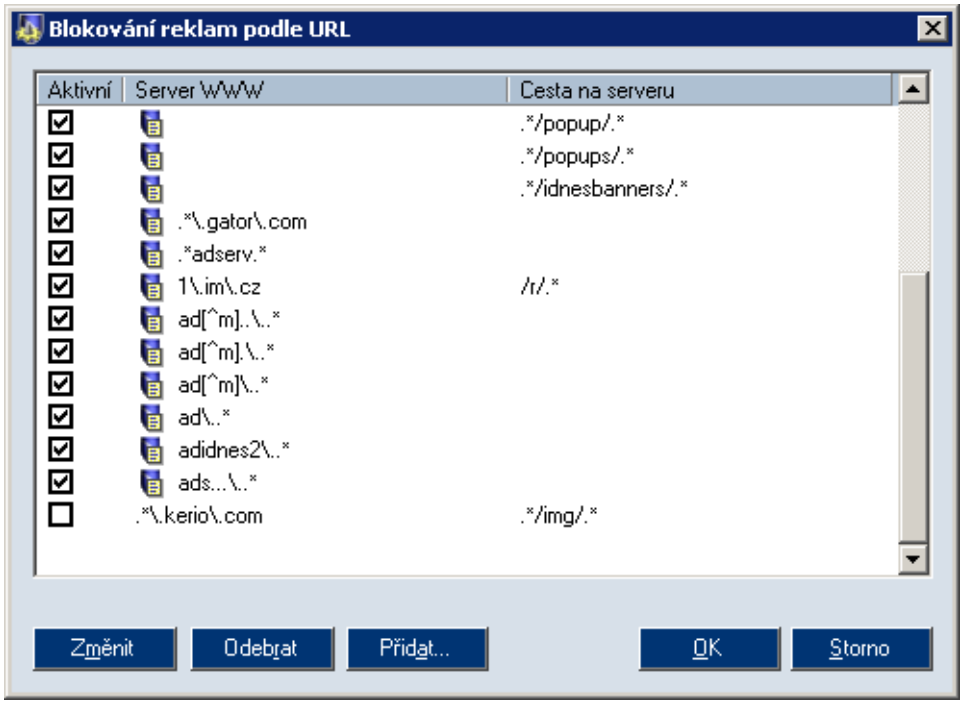
Pravidla pro filtrování reklam

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



Obrázek 14.3 Pravidla pro blokování reklam

- 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).

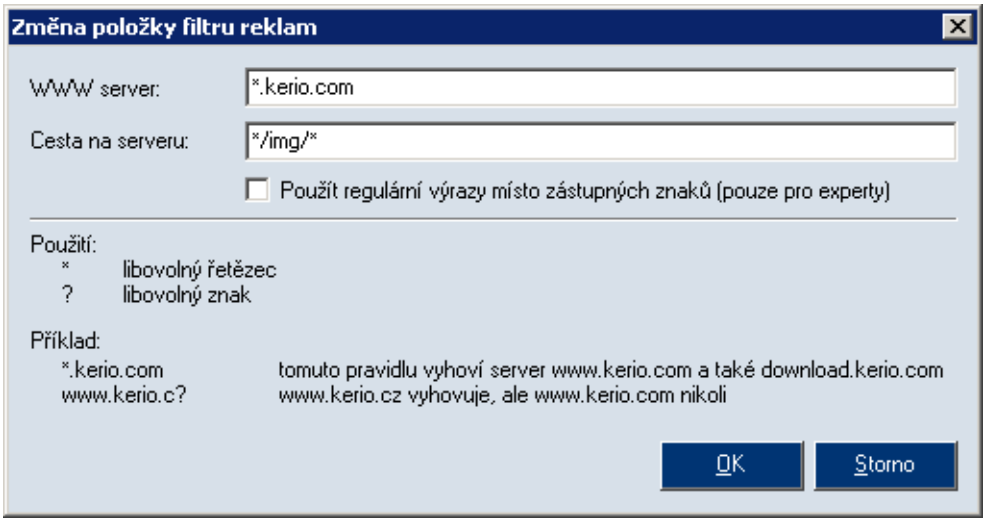
Tlačítko *Přidat* nebo *Změnit* otevírá dialog pro definici pravidla filtru reklam. Pravidlo sestává ze dvou částí:

- *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



Obrázek 14.4 Definice pravidla filtru reklam — použití zástupných znaků

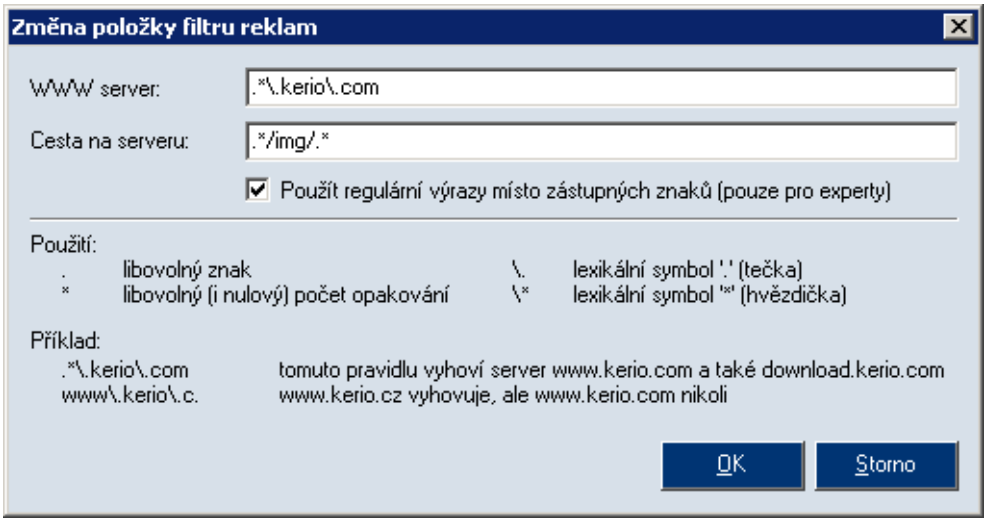
Je-li volba *Použít regulární výrazy místo zástupných znaků* vypnuta, pak lze v položkách *WWW server* a *Cesta na serveru* použít tyto dva zástupné znaky:

- `*` (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



Obrázek 14.5 Definice pravidla filtru reklam — použití regulárních výrazů

Je-li zapnuta volba *Použít regulární výrazy místo zástupných znaků*, musí 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):

- V položce *WWW server* je uveden výraz `.*\.kerio\.com`.

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

- V položce *Cesta na serveru* je uveden výraz `.*/img/.*`.

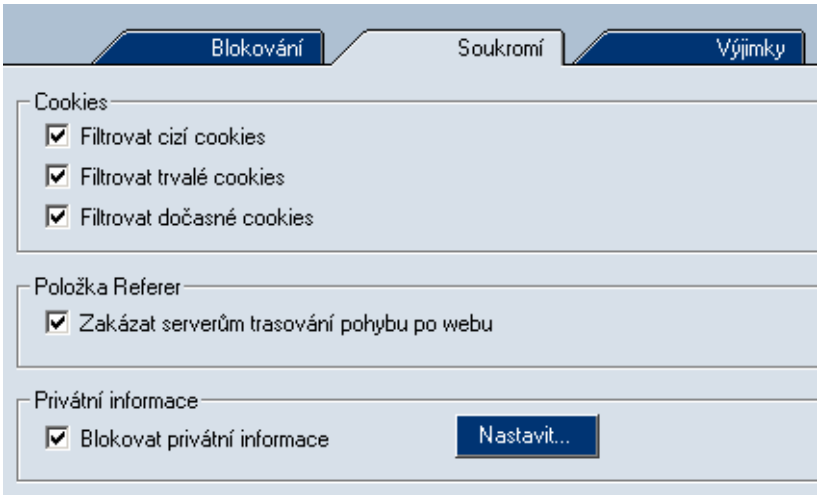
  To znamená, že relativní adresa objektu na serveru musí obsahovat podřetězec `/img/` — tedy např. `/img/banner.gif`, `/data/img/bar.jpg` nebo pouze `/img/`.

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

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

14.2 Ochrana soukromí uživatele

Záložka *Soukromí* obsahuje tyto možnosti ochrany soukromí uživatele:



Obrázek 14.6 Sekce *WWW / Soukromí* — ochrana proti sledování uživatele a úniku privátních informací

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 všechna dočasná cookies smazána.

Poznámka: I v případě, kdy je zapnuto filtrování všech typů cookies, může za určitých okolností dojít k uložení cookie. Typickým příkladem je cookie ukládané skriptem na WWW stránce — pak se nejedná o síťovou komunikaci a *Kerio Personal Firewall* tuto akci nezachytí. Filtrování cookies však nepovolí odeslat žádná cookies na server, čímž uložené cookie ztrácí svůj smysl. Firewall tedy zajišťuje ochranu soukromí uživatele i v těchto případech.

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.

Poznámka: Blokování položky `Referer` může způsobit částečnou nefunkčnost některých WWW stránek. Některé servery totiž mohou používat tuto položku např. pro kontrolu, zda nejsou prvky stránek (obrázky, rámce apod.) využívány jinými servery. Blokování položky `Referer` může mít pak za následek např. zobrazení stránky bez obrázků.

Ve výše uvedených případech doporučujeme definovat výjimky pro konkrétní WWW servery (viz kapitola 14.3).

Blokovat privátní informace

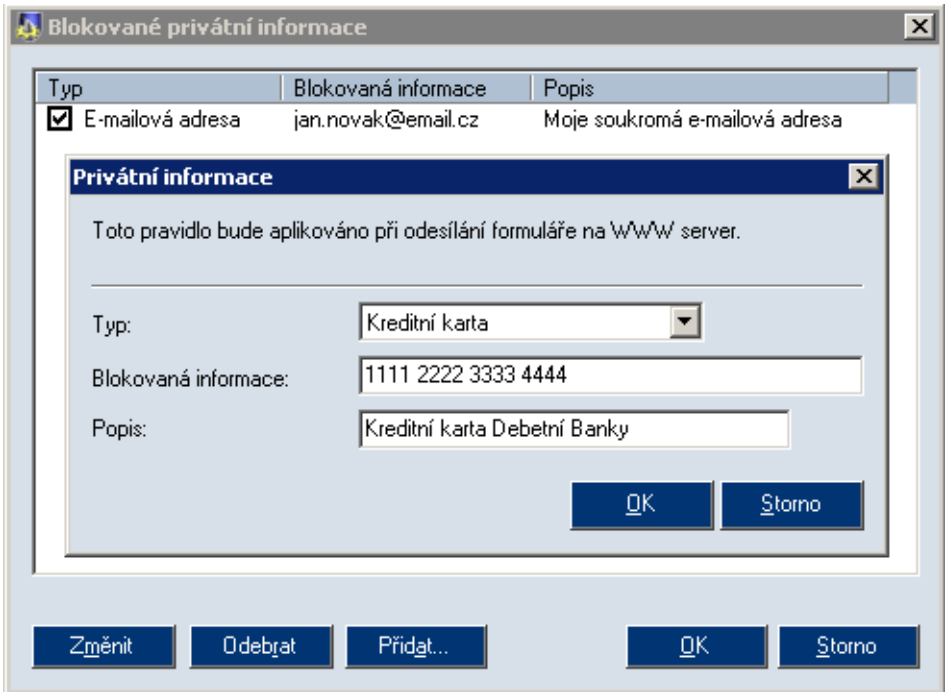
Zákaz odesílání definovaných privátních informací z formulářů na WWW stránkách.

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.



Obrázek 14.7 Definice privátních informací

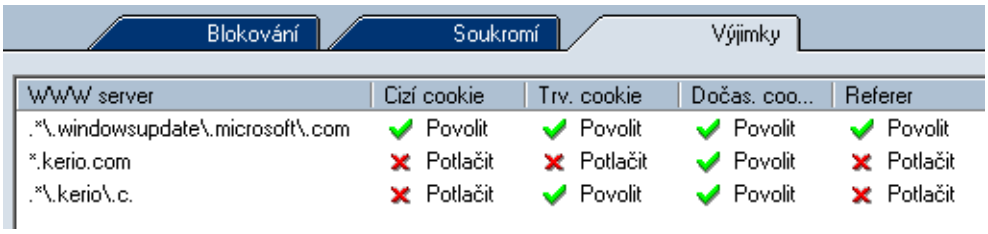
- *Blokovaná informace* — vlastní informace, tj. řetězec, jehož odeslání bude *Kerio Personal Firewall* blokovat.

  Upozornění: V privátních informacích nejsou rozlišována malá a velká písmena.

- *Popis* — popis privátní informace (libovolný text, slouží pro zvýšení přehlednosti).

14.3 Výjimky pro jednotlivé WWW servery

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

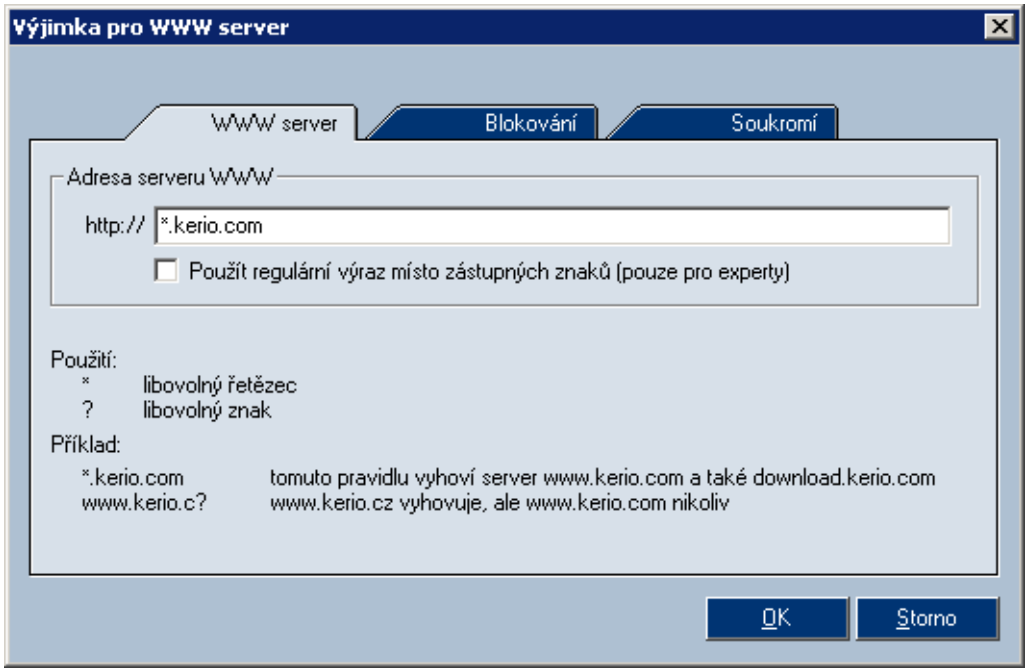


Obrázek 14.8 Sekce *WWW / Výjimky* — specifická nastavení pro konkrétní WWW servery

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.

Záložka *Výjimky* obsahuje jedno předdefinované pravidlo. Toto pravidlo se týká automatických aktualizací společnosti *Microsoft* a povoluje aktualizace ze serveru `windowsupdate.microsoft.com`.

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



Obrázek 14.9 Definice výjimky pro WWW server

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 14.1).

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

Kapitola 15

Stavové informace

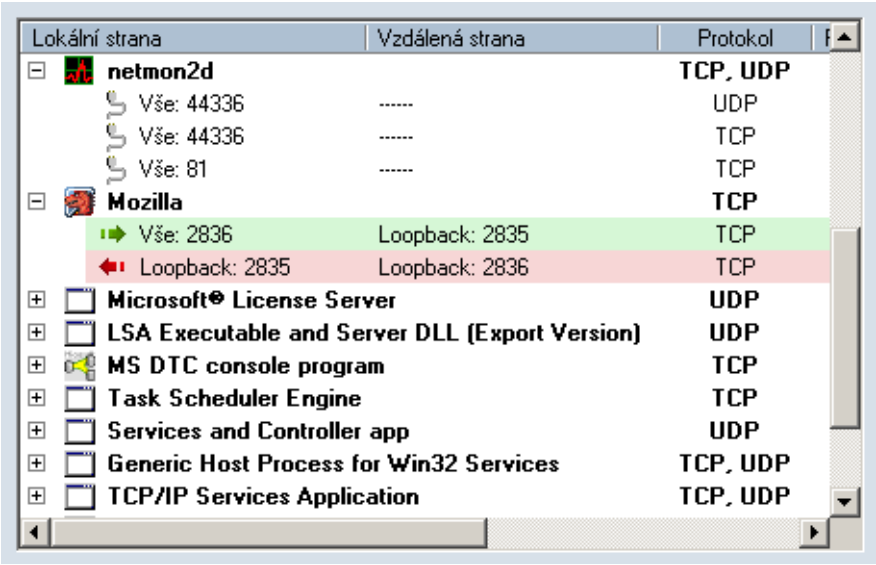
15.1 Přehled spojení a otevřených portů

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 alespoň jeden port.



Obrázek 15.1 Sekce *Přehled / Spojení* — přehled navázaných spojení a otevřených portů dle jednotlivých aplikací

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).

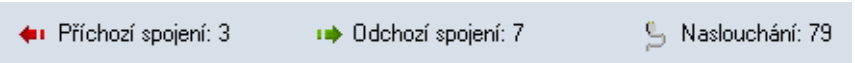
Rychlost příchozí, Rychlost odchozí
: Aktuální rychlost přijímaných (příchozích) a odesílaných (odchozích) dat v rámci daného spojení. Rychlost je uváděna v kilobytech za sekundu (KB/s).

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:

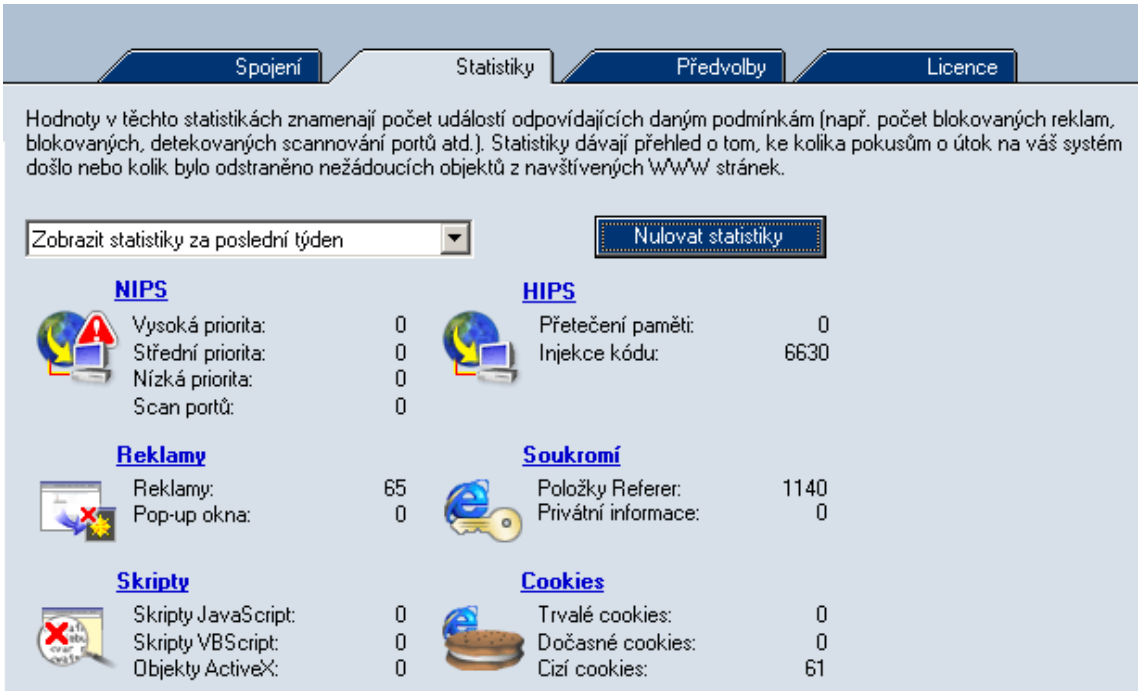


Obrázek 15.2 Sekce *Přehled / Spojení* — celkový počet navázaných spojení a otevřených portů

- *Příchozí 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

15.2 Statistiky

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



Obrázek 15.3 Sekce *Přehled / Statistiky* — statistika blokovaných útoků a nežádoucích prvků WWW stránek

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

- poslední hodina

- poslední den
- poslední týden
- poslední měsíc

Tlačítko *Nulovat statistiky* provede vynulování všech sledovaných statistik. *Kerio Personal Firewall* se po stisknutí tohoto tlačítka dotáže uživatele, zda si skutečně přeje statistiky vynulovat.

Statistiky jsou rozděleny do skupin podle typu. Kliknutím na název skupiny se zobrazí odpovídající záznam (*WWW* (kapitola 16.8), *HIPS* (kapitola 12) nebo *NIPS* (kapitola 16.5).

NIPS

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*)

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

HIPS

Počet detekovaných útoků:

- *Přetečení paměti* — počet pokusů o útok typu buffer overflow.
- *Injekce kódu* — počet pokusů o injekci kódu.

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 16

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`).

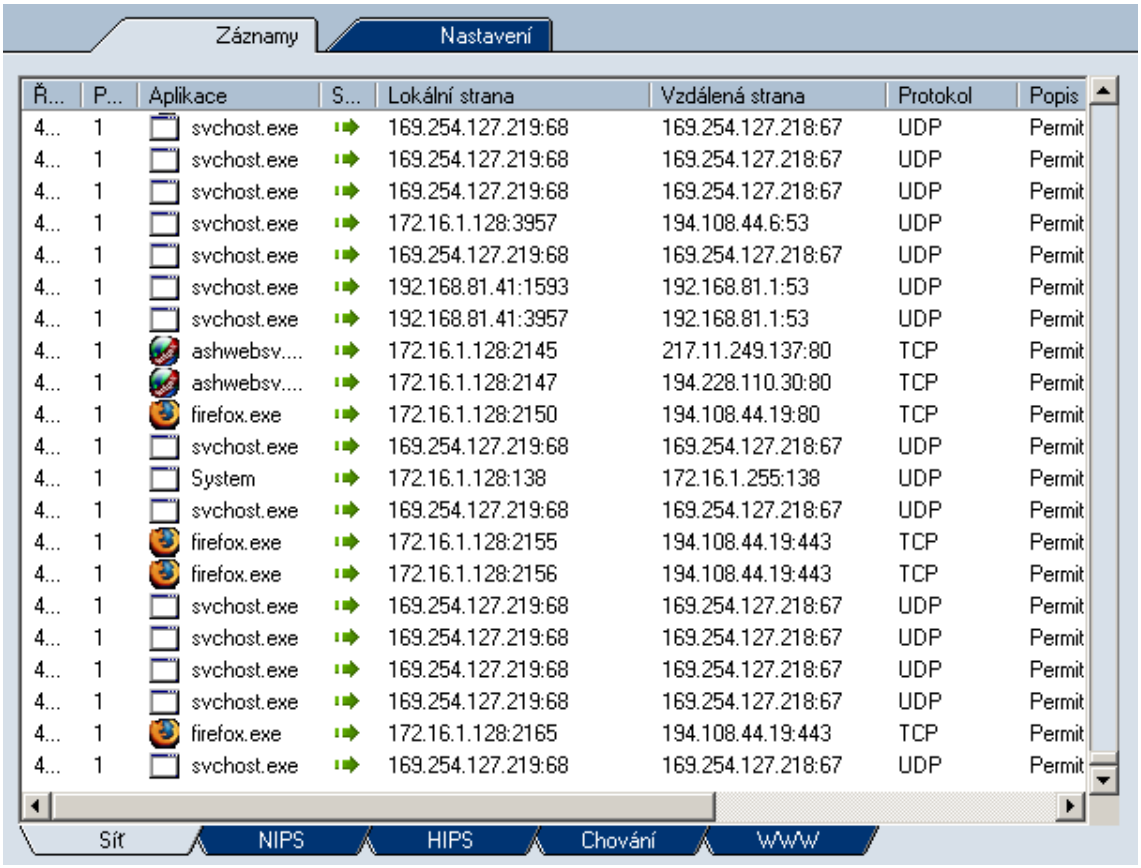
16.1 Prohlížení záznamů

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.



Obrázek 16.1 Sekce *Záznamy* — prohlížení záznamu

- Při řazení podle vybraného sloupce je seřazena pouze aktuálně zobrazená část záznamu. Po přesunu na jinou část záznamu je třeba zobrazené informace znovu seřadit.

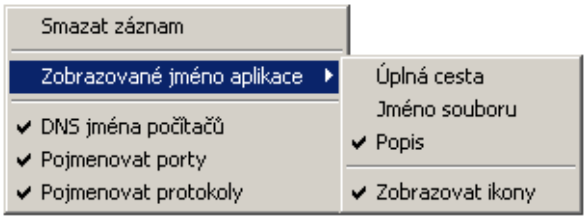
Poznámka: Záznamy *Error*, *Warning* a *Debug* nejsou z uživatelského rozhraní *Kerio Personal Firewall* přístupné — lze je prohlížet pouze jako soubory.

16.2 Kontextové menu pro záznamy

Při stisknutí 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.



Obrázek 16.2 Sekce *Záznamy* — kontextové menu pro záznam Síť

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`).

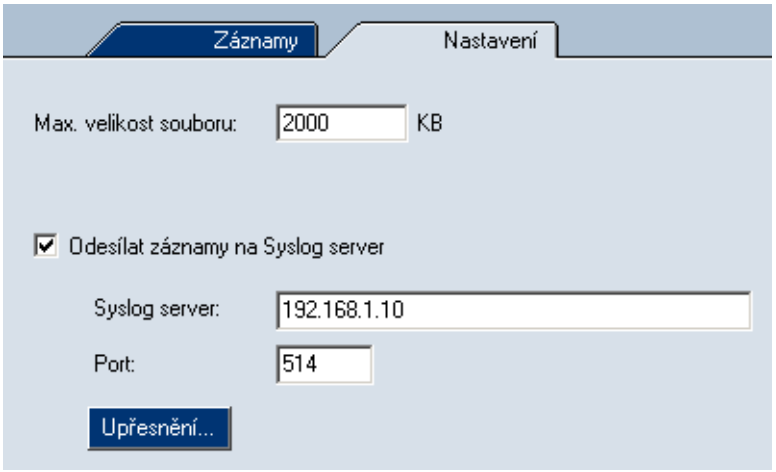
Poznámky:

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 15.1), dialogy *Upozornění na spojení* (kap. 5.2) a *Spouštění/Záměna/Spouštění jiné aplikace* (kap. 5.3) a okno s upozorněním (kap. 5.5). Nastavení zobrazování je rovněž popsáno v příslušných kapitolách.

16.3 Volby pro záznamy

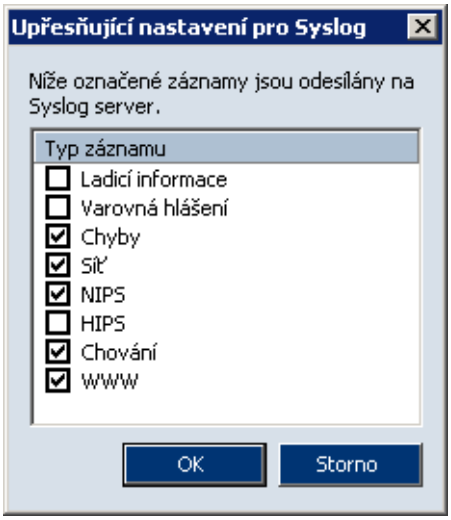
V záložce *Nastavení* sekce *Záznamy* lze nastavit následující parametry a volby pro záznamy (nastavení platí pro všechny záznamy *Kerio Personal Firewallu*):



Obrázek 16.3 Sekce *Záznamy / Nastavení* — max. velikost souboru záznamu

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.

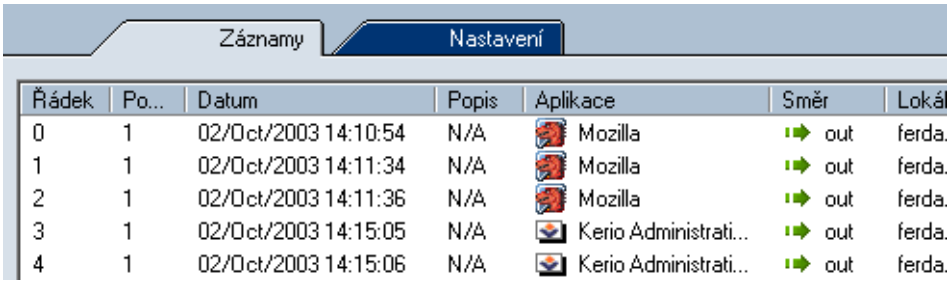


Obrázek 16.4 Nastavení záznamů odesílaných na Syslog server

16.4 Záznam Síť

Do záznamu *Network* se ukládají informace o síťové komunikaci, která vyhověla určitému pravidlu pro aplikaci (viz kapitola 7.2) nebo pravidlu paketového filtru (viz kapitola 8). Komunikace se zaznamenává pouze tehdy, pokud je v příslušném pravidle zapnuta volba *Zaznamenat komunikaci do záznamu Síť*.

Záznam *Síť* obsahuje tyto informace:



Obrázek 16.5 Sekce *Záznamy* — záznam *Síť*

- *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

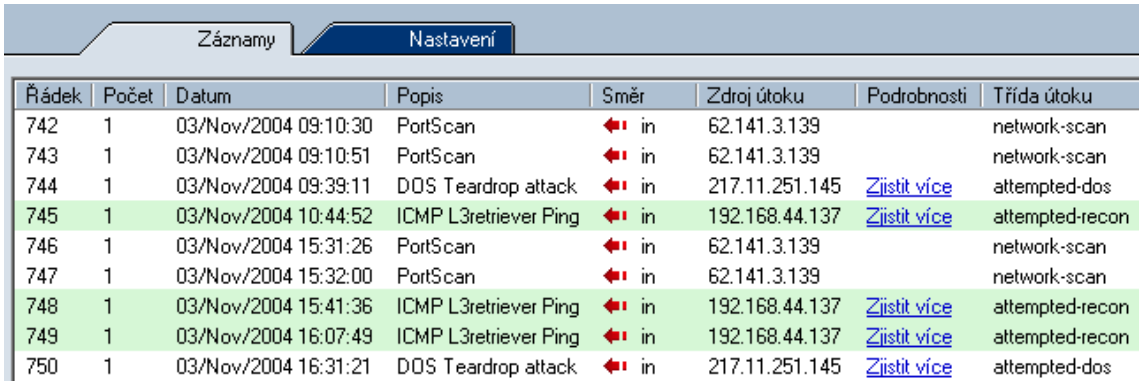
  Poznámka: Do souboru záznamu je ukládán jak popis aplikace, tak úplná cesta ke spustitelnému souboru. Proto lze v okně záznamu způsob zobrazení aplikace libovolně přepínat.
- *Směr* — směr navázání spojení (*in* = na lokální počítač, *out* = z lokálního počítače)
- *Lokální strana* — lokální IP adresa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

16.5 Záznam NIPS

Do záznamu *NIPS* se zapisují informace o detekovaných síťových útocích. Zaznamenávány jsou útoky těch skupin, u nichž je zapnuta volba *Zaznamenat* (viz kapitolu 11). Síťové útoky, které byly detekovány, ale nebyly blokovány, jsou zvýrazněny zelenou barvou (jedná se o útoky patřící do prioritní třídy, která není blokována — viz kapitola 11.1).

Každý řádek záznamu *NIPS* obsahuje tyto informace:

- *Řádek* — číslo řádku záznamu



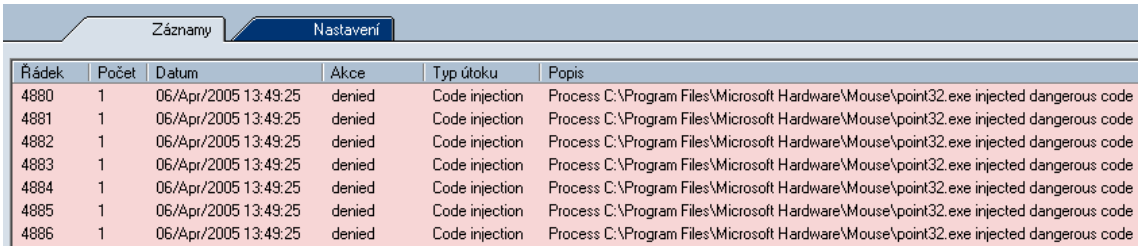
Řádek	Počet	Datum	Popis	Směr	Zdroj útoku	Podrobnosti	Třída útoku
742	1	03/Nov/2004 09:10:30	PortScan	in	62.141.3.139		network-scan
743	1	03/Nov/2004 09:10:51	PortScan	in	62.141.3.139		network-scan
744	1	03/Nov/2004 09:39:11	DOS Teardrop attack	in	217.11.251.145	Zjistit více	attempted-dos
745	1	03/Nov/2004 10:44:52	ICMP L3retriever Ping	in	192.168.44.137	Zjistit více	attempted-recon
746	1	03/Nov/2004 15:31:26	PortScan	in	62.141.3.139		network-scan
747	1	03/Nov/2004 15:32:00	PortScan	in	62.141.3.139		network-scan
748	1	03/Nov/2004 15:41:36	ICMP L3retriever Ping	in	192.168.44.137	Zjistit více	attempted-recon
749	1	03/Nov/2004 16:07:49	ICMP L3retriever Ping	in	192.168.44.137	Zjistit více	attempted-recon
750	1	03/Nov/2004 16:31:21	DOS Teardrop attack	in	217.11.251.145	Zjistit více	attempted-dos

Obrázek 16.6 Sekce *Záznamy* — záznam *NIPS*

- *Počet* — počet identických zpráv
- *Datum* — datum a čas zápisu zprávy do záznamu
- *Popis* — název (popis) zachyceného útoku (viz kapitola 11.1)
- *Směr* — směr útoku (útok může být veden i z lokálního počítače)
- *Zdroj útoku* — IP adresa (resp. jméno) vzdáleného počítače (pokud je zjistitelná — útok může být veden z falšované IP adresy)
- *Podrobnosti* — odkaz na WWW stránku s bližšími informacemi o útoku (jsou-li k dispozici)
- *Třída útoku* — třída, do které je útok klasifikován (viz kapitola 11.1)
- *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)

16.6 Záznam HIPS

Do záznamu *HIPS* se zapisují informace o detekovaných útocích na aplikace. Zaznamenávány jsou útoky těch skupin, u nichž je zapnuta volba *Zaznamenat pokusy do záznamu HIPS* (viz kapitolu 12). Detekované útoky, které však nebyly blokovány, jsou značeny bílou barvou, zablokované útoky jsou označeny červeně.



Řádek	Počet	Datum	Akce	Typ útoku	Popis
4880	1	06/Apr/2005 13:49:25	denied	Code injection	Process C:\Program Files\Microsoft Hardware\Mouse\point32.exe injected dangerous code
4881	1	06/Apr/2005 13:49:25	denied	Code injection	Process C:\Program Files\Microsoft Hardware\Mouse\point32.exe injected dangerous code
4882	1	06/Apr/2005 13:49:25	denied	Code injection	Process C:\Program Files\Microsoft Hardware\Mouse\point32.exe injected dangerous code
4883	1	06/Apr/2005 13:49:25	denied	Code injection	Process C:\Program Files\Microsoft Hardware\Mouse\point32.exe injected dangerous code
4884	1	06/Apr/2005 13:49:25	denied	Code injection	Process C:\Program Files\Microsoft Hardware\Mouse\point32.exe injected dangerous code
4885	1	06/Apr/2005 13:49:25	denied	Code injection	Process C:\Program Files\Microsoft Hardware\Mouse\point32.exe injected dangerous code
4886	1	06/Apr/2005 13:49:25	denied	Code injection	Process C:\Program Files\Microsoft Hardware\Mouse\point32.exe injected dangerous code

Obrázek 16.7 Sekce *Záznamy* — záznam *HIPS*

- *Řádek* — číslo řádku záznamu
- *Počet* — počet identických zpráv
- *Datum* — datum a čas zápisu zprávy do záznamu
- *Akce* — akce, kterou *Kerio Personal Firewall* provedl při zachycení tohoto útoku (*permitted* — útok povolen, *denied* — útok zakázán)
- *Typ útoku* — název zachyceného útoku (viz kapitolu 12)

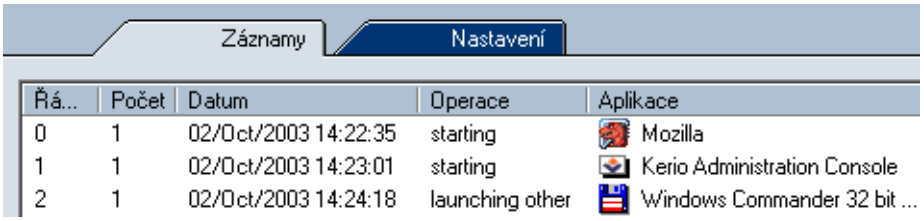
Z následujících tří položek lze v kontextovém menu (nabídka pravého tlačítka myši) vybrat vždy jen jednu možnost zobrazení informace:

- *Popis* — popis útoku.
- *Úplná cesta* — položka bude obsahovat informaci o úplné cestě k útočící i napadané aplikaci.
- *Jméno souboru* — jméno napadeného souboru.

16.7 Záznam Chování

Do záznamu *Chování* se zapisují informace o spouštění aplikací, které vyhovují určitým pravidlům v sekci *Útoky → Blokování chování aplikací*. Záznam se provádí pouze tehdy, je-li v příslušném pravidle zapnuta volba *Zaznamenat do záznamu Chování*.

Záznam *Systém* obsahuje tyto informace:



Obrázek 16.8 Sekce *Záznamy* — záznam *Chování*

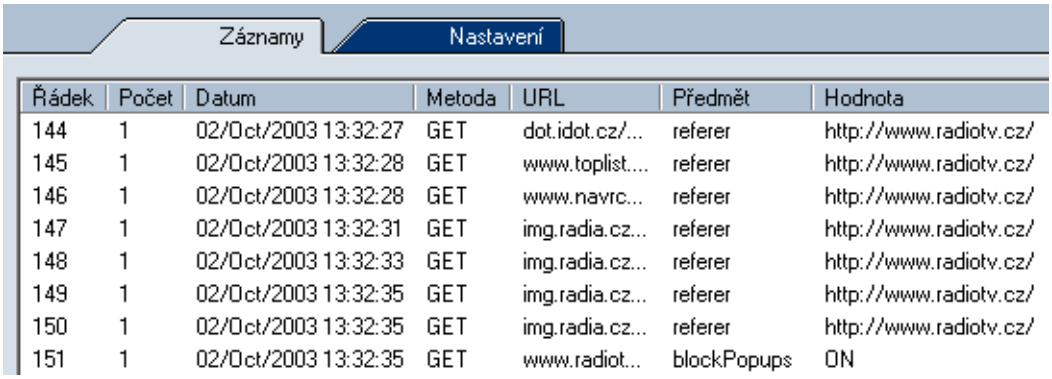
- *Řádek* — číslo řádku záznamu
- *Počet* — počet identických zpráv
- *Datum* — datum a čas zápisu zprávy do záznamu
- *Operace* — typ operace:
  1. *starting* — spouštění aplikace
  2. *starting modified* — změna ve spustitelném souboru aplikace
  3. *launching other* — aplikace spouští jinou aplikaci
- *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:
  1. *permitted* — spuštění aplikace povoleno
  2. *denied* — spuštění aplikace zakázáno
  3. *asked* → *permitted* — zobrazen dotaz uživateli
     (tj. dialog *Spouštění/Záměna/Spouštění jiné aplikace*), uživatel spuštění povolil
  4. *asked* → *denied* — zobrazen dotaz uživateli, uživatel spuštění zakázal

16.8 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 14), zaznamenávají se všechny filtrované objekty.

Záznam *WWW* obsahuje tyto informace:

- *Řádek* — číslo řádku záznamu



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

Obrázek 16.9 Sekce *Záznamy* — záznam *WWW*

- *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 14.1)
- 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.

16.9 Záznamy Debug, Error a Warning

Záznamy *Error*, *Warning* a *Debug* nejsou z uživatelského rozhraní *Kerio Personal Firewall* přístupné — lze je prohlížet pouze jako soubory v podadresáři `Logs` adresáře, kam byl *Kerio Personal Firewall* nainstalován (typicky `C:\Program Files\Kerio\Personal Firewall 4\logs`). Vlastní soubor záznamu má příponu `.log` (např. `error.log`).

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).

Příloha A

Použité open-source knihovny

Produkt *Kerio Personal Firewall* obsahuje následující knihovny volně šiřitelné ve formě zdrojových kódů (open-source):

libiconv

Knihovna pro konverzi kódování znaků s použitím konverze z/do Unicode.
Copyright ©1999-2003 Free Software Foundation, Inc.
Autor: Bruno Haible

OpenSSL

Implementace protokolů *Secure Sockets Layer* (SSL v2/v3) a *Transport Layer Security* (TLS v1).
Tento produkt obsahuje software vyvinutý sdružením *OpenSSL Project* pro použití v *OpenSSL Toolkit* (`http://www.openssl.org/`).

zlib

Všestranně použitelná knihovna pro kompresi a dekompresi dat.
Copyright ©1995-2003 Jean-Loup Gailly and Mark Adler.

Slovníček pojmů

ActiveX objekt
: Proprietární technologie společnosti Microsoft určená k vytváření dynamických objektů na WWW stránkách. Tato technologie poskytuje poměrně široké možnosti, mimo jiné zápis na disk nebo spouštění příkazů na klientovi (tj. počítači, na kterém byla otevřena příslušná WWW stránka). Viry nebo červy dokáží prostřednictvím technologie *ActiveX* např. změnit telefonní číslo vytáčené linky.

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 mohou být zneužívány pro sledování, které stránky uživatel navštívil, případně k počítání přístupů.

DHCP
: DHCP (Dynamic Host Configuration Protocol) je služba dynamické konfigurace v síti TCP/IP (IP adresa, maska, brána, DNS, atd.).

DNS
: DNS (Domain Name System) je internetová služba distribuované databáze, která slouží pro převod doménových jmen na jim odpovídající IP adresy.

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*.

HTTP

HTTP (HyperText Transfer Protocol) je jednoduchý aplikační protokol, který slouží k přenosu webových dokumentů a obrázků.

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.

IP adresa

32-bitové číslo jednoznačně určující počítač v Internetu. Zapisuje v desítkové soustavě jako čtveřice bytů (0–255) oddělených tečkami (např. `200.152.21.5`). Každý paket obsahuje informaci, odkud byl vyslán (zdrojová IP adresa), a kam má být doručen (cílová IP adresa).

JavaScrypt

JavaScript je skryptovací jazyk, který představuje výkonný kód na WWW stránce. Tento kód provádí klient (WWW prohlížeč). Skripty slouží k vytváření dynamických prvků na WWW stránkách, mohou však být zneužity pro zobrazování reklam, získávání informací o uživateli apod.

Maska subsítě

Maska subsítě rozděluje IP adresu na dvě části: adresu sítě a adresu počítače v této síti. Maska se zapisuje stejně jako IP adresa (např. 255.255.255.0), ale je třeba ji vidět jako 32-bitové číslo mající zleva určitý počet jedniček a zbytek nul (maska tedy nemůže mít libovolnou hodnotu). Jednička v masce subsítě označuje bit adresy sítě a nula bit adresy počítače. Všechny počítače v jedné subsíti musejí mít stejnou masku subsítě a stejnou síťovou část IP adresy.

NAT

NAT (Network Address Translation — překlad IP adres) představuje záměnu IP adres v paketech procházejících firewallem.

Technologie NAT umožňuje připojení privátní lokální sítě k Internetu přes jedinou veřejnou IP adresu. Všechny počítače v lokální síti mají přímý přístup do Internetu, jako by se jednalo o veřejnou subsíť (platí zde určitá omezení). Zároveň mohou být na veřejné IP adrese mapovány služby běžící na počítačích v lokální síti.

Paket
: Paket neboli IP datagram je základní jednotkou dat v síti IP.

Paketový filtr
: Paketový filtr je aplikace, která kontroluje hlavičky příchozích paketů. Na základě obsahu těchto hlaviček některé pakety propustí do sítě a jiné zahodí.

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.

Proxy server
: Velmi rozšířený způsob sdílení internetového připojení. Proxy server představuje prostředníka mezi klientem a cílovým serverem.
Proxy server pracuje na aplikační úrovni a je přizpůsoben několika aplikačním protokolům (např. HTTP, FTP, Gopher). Ve srovnání s technologií NAT jsou jeho možnosti velmi omezené.

Regulární výraz
: Regulární výrazy (regular expression) jsou speciální jazyky pro popis řetězce.

Síťové rozrhaní
: Obecné označení pro zařízení, které propojuje počítač s ostatními počítači určitým typem komunikačního média. Síťové rozhraní může být např. Ethernet adaptér, TokenRing adaptér nebo modem. Prostřednictvím síťového rozhraní počítač vysílá a přijímá pakety.

Systémový registr
: Systémový registr je speciální soubor obsažený ve všech operačních systémech Windows. Tento soubor obsahuje veškeré nastavení i informace, které OS a instalované programy potřebují pro svou činnost.

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).

Trójský kůň

Aplikace, která slouží k jiným účelům, než prezentuje. Obvykle vypadá jako užitečná, ale obsahuje škodlivý kód.

UDP

UDP (User Datagram Protocol) je tzv. nespojovaný protokol, 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.

URI

URI (Uniform Resource Identifier) je standard popisující umístění objektu na Internetu. Popisuje mechanismus přístupu k objektu (např. protokol), určení počítače (např. DNS, IP), kde je objekt umístěn a umístění objektu na počítači (např. cestu a název souboru). Podmnožinou URI je URL a URN.

URL

URL (Unique Resource Locator) je podmnožinou URI, která jednoznačně popisuje umístění souboru v počítačové síti.

VBScript

Skriptovací jazyk založený na jazyce Visual Basic, který představuje výkonný kód na WWW stránce. Tento kód provádí klient (WWW prohlížeč). Skripty slouží k vytváření dynamických prvků na WWW stránkách, mohou však být zneužity pro zobrazování reklam, získávání informací o uživateli apod.

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* povoluje/zakazuje vytváření VPN protokolem *PPTP* (proprietární protokol firmy *Microsoft*).

VPN

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* povoluje/zakazuje vytváření VPN protokolem *PPTP* (proprietární protokol firmy *Microsoft*).

WWW

World Wide Web (zkráceně WWW nebo web) je v současné době nejpopulárnější služba, která je na Internetu nabízena. Umožňuje přenášet soubory s multimediálním obsahem (texty, zvuky, obrazy).

Rejstřík

N

P

R

S

U

V

Z