Kerio WinRoute Firewall 5™

Příručka administrátora

Kerio Technologies

Datum vydání: 20. 6. 2003

Tento produkt obsahuje kryptografické knihovny vyvinuté v projektu OpenSSL (http://www.openssl.org/), jejichž spoluautorem je Eric Young (eay@cryptsoft.com).

Tento produkt obsahuje knihovny pro adresářové služby vyvinuté v projektu OpenLDAP (http://www.openldap.org/).

Obsah

Kapitola 1

Rychlé nastavení

Tato kapitola obsahuje seznam kroků, které je nutno provést, aby mohl *Kerio WinRoute Firewall* (dále jen *WinRoute*) okamžitě sloužit pro sdílení internetového připojení a ochranu vaší lokální sítě. Podrobný postup rychlé instalace a konfigurace naleznete v samostatném manuálu *WinRoute — Konfigurace krok za krokem*.

Nebudete-li si jisti některým nastavením *WinRoute*, jednoduše vyhledejte příslušnou kapitolu v tomto manuálu. Informace týkající se internetového připojení (IP adresa, výchozí brána, DNS server atd.) vám sdělí váš poskytovatel Internetu.

Poznámka: V následujícím textu je termínem *firewall* označován počítač, kde je *WinRoute* nainstalován (resp. kam má být nainstalován).

1. Firewall musí mít alespoň dvě rozhraní — jedno připojené do lokální sítě (např. síťová karta *Ethernet* nebo *Token Ring*) a jedno připojené do Internetu (např. analogový modem, ISDN adaptér, síťová karta nebo DirecPC adaptér). Na obou (resp. všech) rozhraních musí být správně nastaveny parametry TCP/IP.

   Před zahájením instalace *WinRoute* prověřte komunikaci s počítači v lokální síti a funkčnost internetového připojení. Tímto testem si ušetříte mnoho problémů při pozdějším ladění konfigurace a hledání chyb.

2. Spusťte instalaci *WinRoute*. V průvodci počáteční konfugurací zadejte uživatelské jméno a heslo pro přístup ke správě (podrobnosti viz kapitoly 2.3 a 2.8).

3. Nastavte základní komunikační pravidla pomocí *Průvodce komunikačními pravidly* (viz kapitola 5.1).

4. Zapněte *DHCP server* a nastavte požadované rozsahy IP adres včetně parametrů (maska subsítě, výchozí brána, adresa DNS serveru, příp. jméno domény). Podrobnosti viz kapitola 4.3.

5. Zkontrolujte nastavení *DNS Forwarderu*. Chcete-li prohledávat soubor `hosts` a/nebo tabulky DHCP serveru, nezapomeňte uvést lokální DNS doménu. Podrobnosti viz kapitola 4.2.

6. Vytvořte nebo importujte uživatelské účty a skupiny, nastavte požadovaná přístupová práva a zařaďte účty do skupin. Podrobnosti viz kapitoly 9.1 a 9.2.

7. Definujte skupiny IP adres (kap. 8.1), časové intervaly (kap. 8.2) a skupiny URL (kap. 8.4), které použijete při definici pravidel (viz kap. 8.2).

8. Vytvořte pravidla pro URL (kap. 6.1) a nastavte systém *Cobion Orange Filter* (kap. 6.3). Nastavte HTTP cache a automatickou konfiguraci prohlížečů (kap. 4.5). Definujte pravidla pro FTP (kap. 6.5).

9. Vyberte antivirový program a nastavte typy objektů, které mají být kontrolovány. Jedná-li se o integrovaný antivirus *McAfee*, zkontrolujte a případně upravte nastavení automatické aktualizace.

   Poznámka: Externí antivirový program musí být nainstalován dříve, než jej ve *WinRoute* zvolíte.

10. Nastavte parametry TCP/IP síťového adaptéru každé klientské stanice v lokální síti jedním z následujících způsobů:

    - *Automatická konfigurace* — zapněte volbu *Získávat IP adresu automaticky* (*Obtain an IP address automatically*). Nenastavujte žádné další parametry.

    - *Ruční konfigurace* — zadejte IP adresu, masku subsítě, adresu výchozí brány, adresu DNS serveru a jméno lokální domény.

    Na každé stanici nastavte WWW prohlížeč jedním z těchto způsobů:

    - *Automatická konfigurace* — zaškrtněte volbu *Automaticky zjišťovat nastavení* (*Microsoft Internet Explorer*) nebo zadejte URL pro automatickou konfiguraci (jiné typy prohlížečů). Podrobnosti naleznete v kapitole 4.5.

    - *Ruční konfigurace* — zvolte připojení lokální sítí, případně nastavte IP adresu a port proxy serveru (viz kapitola 4.4).

Kapitola 2

Úvod

2.1 Kerio WinRoute Firewall 5.0

WinRoute je komplexní nástroj pro připojení lokální sítě do Internetu a její ochranu proti průniku zvenčí. Je určen pro platformy Windows NT 4.0, 2000 a XP.

Základní vlastnosti aplikace *WinRoute*:

Transparentní přístup do Internetu Díky technologii NAT (Network Address Translation — překlad IP adres) je možné připojit lokální privátní síť do Internetu přes jedinou veřejnou IP adresu (statickou i dynamickou). Narozdíl od klasického proxy serveru budou mít všechny počítače plný přístup do Internetu a bude na nich možné provozovat většinu běžných síťových aplikací, jako by se jednalo o veřejnou síť, která je součástí Internetu.

Bezpečnost Integrovaný firewall ochrání celou lokální síť včetně počítače, na němž je nainstalován. Nezáleží na tom, zda je použita funkce NAT (překlad IP adres) nebo zda je *WinRoute* nasazen jako „neutrální“ směrovač mezi dvěma sítěmi. *WinRoute* poskytuje ochranu srovnatelnou s mnohonásobně dražšími hardwarovými firewally.

Obsluha protokolů (inspekční moduly) Některé aplikace komunikují netriviálním způsobem — např. vyžadují otevření dalšího spojení serverem zpět na klienta, používají nestandardní komunikační protokoly apod. Aby bylo možné za firewallem provozovat i takovéto aplikace, obsahuje *WinRoute* tzv. inspekční moduly, které rozpoznají příslušný aplikační protokol a dokáží dynamicky přizpůsobit chování firewallu (např. dočasné otevření spojení, které si aplikace vyžádala). Jako příklad uveďme FTP v aktivním režimu, RealAudio nebo PPTP.

Řízení přístupu Veškerá bezpečnostní nastavení jsou ve *WinRoute* realizována prostřednictvím tzv. komunikačních pravidel. Ta umožňují nejen ochránit síť proti průniku zvenčí, ale také zpřístupnit služby běžící na serverech uvnitř chráněné lokální sítě (např. WWW server, poštovní server, FTP server atd.) z Internetu nebo naopak omezit přístup lokálních uživatelů k určitým službám v Internetu.

Filtrování obsahu *WinRoute* umožňuje sledovat obsah komunikace protokoly HTTP a FTP a blokovat objekty (stránky, přesměrování, některé prvky HTML atd.), které nevyhovují zadaným kritériím. Tato nastavení mohou být globální nebo specifická pro

konkrétní uživatele. Stahované objekty mohou být také transparentně kontrolovány externím antivirovým programem.

Konfigurace sítě *WinRoute* obsahuje vestavěný DHCP server, který automaticky nastaví parametry TCP/IP na všech počítačích (pracovních stanicích) ve vaší lokální síti. Veškeré parametry stačí nastavit centrálně na serveru. Tím se jednak ušetří čas potřebný ke zprovoznění sítě a jednak sníží riziko možných chyb.

Ke snadné konfiguraci DNS a zrychlení odpovědí na DNS dotazy slouží modul *DNS forwarder*. Jedná se o jednoduchý DNS server (caching nameserver), který předává dotazy jinému DNS serveru. Získané odpovědi ukládá do své vyrovnávací paměti (cache) — odezvy na opakované dotazy jsou tak mnohonásobně rychlejší. Ve spolupráci s DHCP serverem a systémovým souborem `hosts` může zároveň fungovat jako dynamický DNS server pro lokální doménu.

Vzdálená správa Veškerá nastavení *WinRoute* se provádějí v odděleném programu *Kerio Administration Console* (univerzální administrační konzola pro serverové produkty firmy Kerio Technologies). Tento program může být provozován jak přímo na počítači, kde je *WinRoute* nainstalován, tak na libovolném jiném počítači ve vaší lokální síti či v Internetu. Komunikace mezi *WinRoute* a administračním programem je šifrována a nemůže tedy dojít k jejímu odposlechu a zneužití.

Různé operační systémy v lokální síti *WinRoute* pracuje s protokoly standardu TCP/IP a z pohledu počítačů v lokální síti se chová jako standardní směrovač. Na tyto počítače není třeba instalovat žádný speciální software, a může zde být provozován libovolný operační systém podporující TCP/IP (např. Windows, Unix/Linux, Mac OS atd.).

Poznámka: WinRoute pracuje pouze s protokolovou sadou TCP/IP. Na funkci jiných protokolů (např. IPX/SPX, NetBEUI, AppleTalk apod.) nemá žádný vliv.

2.2 Konfliktní software

Počítač, na němž je *WinRoute* nainstalován, může být rovněž využíván jako pracovní stanice (to ale není příliš doporučováno — činnost uživatele může mít negativní vliv na chod operačního systému a tím i *WinRoute*).

WinRoute může být provozován společně s většinou běžných aplikací. Existují však určité aplikace, které mohou vykazovat kolize, a neměly by proto být na tomtéž počítači provozovány.

Kolize nízkoúrovňových ovladačů *WinRoute* vykazuje kolize s aplikacemi, jejichž nízkoúrovňové ovladače používají stejnou nebo podobnou technologii, což jsou zejména:

- Aplikace pro sdílení Internetového připojení — např. *Microsoft Internet Connection Sharing (ICS — Sdílení internetového připojení)* (součást novějších verzí Windows), *Microsoft Proxy Server* a *Microsoft Proxy Client* apod.
- Síťové firewally — např. *Microsoft ISA Server*, *CheckPoint Firewall-1*, *WinProxy* firmy Ositis, *Sygate Office Network* a *Sygate Home Network* apod.
- Osobní firewally — např. *Kerio Personal Firewall*, *Internet Connection Firewall* (součást Windows XP), *Zone Alarm*, *Sygate Personal Firewall*, *Norton Personal Firewall* apod.
- Software pro vytváření virtuálních privátních sítí (VPN) — např. firem CheckPoint, Cisco Systems, Nortel apod. Těchto aplikací existuje celá řada a vyznačují se velmi specifickými vlastnostmi, které se liší u jednotlivých výrobců. Konkrétní VPN server či VPN klienta doporučujeme otestovat se zkušební verzí *WinRoute* a případně kontaktovat technickou podporu firmy *Kerio Technologies* (viz `http://www.kerio.cz/`).

  Poznámka: Implementace VPN obsažená v operačním systému Windows (založená na protokolu PPTP firmy Microsoft) je ve *WinRoute* podporována.

Kolize portů Na počítači, kde je *WinRoute* nainstalován, nemohou být provozovány aplikace, které využívají tytéž porty (nebo je třeba konfiguraci portů změnit). Pokud jsou zapnuty všechny služby, využívá *WinRoute* tyto porty:

- `53/UDP` — *DNS Forwarder*
- `67/UDP` — *DHCP server*
- `1900/UDP` — služba *SSDP Discovery*
- `2869/TCP` — služba *UPnP Host*

  Výše uvedené dvě služby jsou součásti podpory protokolu UPnP (viz kapitola 10.5).
- `4080/TCP` — WWW administrační rozhraní (viz kapitola 7)
- `4081/TCP` — zabezpečená (SSL) verze WWW administračního rozhraní (viz kapitola 7)

- `3128/TCP` — HTTP proxy server (viz kapitola 4.4)
- `44333/TCP+UDP` — komunikace mezi programem *Kerio Administration Console* a *WinRoute Firewall Engine*. Tuto službu jako jedinou nelze vypnout ani změnit její port.

Antivirové programy Je-li na počítači s *WinRoute* nainstalován antivirový program, který provádí průběžnou automatickou kontrolu souborů na disku, je třeba z kontroly vyloučit adresář HTTP cache (viz kapitola 4.5, standardně podadresář `cache` adresáře, kde je *WinRoute* nainstalován) a podadresář `tmp` (používá se pro antivirovou kontrolu HTTP a FTP objektů). Jestliže je antivirová kontrola spouštěna pouze ručně, nemusí být tyto adresáře z kontroly vyloučeny — pak je ale nutné před spuštěním antivirové kontroly zastavit *WinRoute Firewall Engine* (což nemusí být vždy vhodné).

Poznámka: Pokud *WinRoute* využívá antivirový program pro kontrolu objektů stahovaných protokoly HTTP a FTP (viz kapitola 6.6), pak vyloučení adresáře cache z kontroly souborů na disku nepředstavuje žádnou hrozbu — soubory uložené v tomto adresáři jsou již antivirovým programem zkontrolovány.

2.3 Instalace

Systémové požadavky

Minimální hardwarová konfigurace počítače, na který má být *WinRoute* nainstalován:

- CPU Intel Pentium II nebo kompatibilní; 300 MHz
- 128 MB operační paměti RAM
- Dvě síťová rozhraní (včetně vytáčených)
- 8 MB diskového prostoru pro instalaci
- Diskový prostor pro logy (dle intenzity provozu a zvolené úrovně logování)

Instalaci je možné provést na tyto operační systémy:

- Windows 98
- Windows Me
- Windows NT 4.0

- Windows 2000
- Windows XP
- Windows Server 2003

Poznámka: Plně podporovány jsou operační systémy Windows NT 4.0, 2000, XP a Server 2003. V případě Windows 98 a Me nezaručujeme 100% funkčnost z důvodu odlišnosti a nestability těchto systémů.

Upozornění: V systémech Windows NT, 2000, XP a Server 2003 musí být nainstalována síťová komponenta *Klient sítě Microsoft* (*Client for Microsoft Networks*), jinak nebude možné provozovat *WinRoute* jako službu.

Kroky před spuštěním instalace

WinRoute by měl být nainstalován na počítač, který tvoří bránu mezi lokální sítí a Internetem. Tento počítač musí obsahovat alespoň jedno rozhraní připojené do lokální sítě (Ethernet, TokenRing apod.) a rozhraní do Internetu. Internetovým rozhraním může být buď síťový adaptér (Ethernet, WaveLAN atd.) nebo modem (analogový, ISDN apod.).

Před zahájením instalace *WinRoute* doporučujeme prověřit následující:

- Správné nastavení systémového času (nutné pro kontrolu aktualizací operačního systému, antivirového programu atd.)
- Instalaci všech nejnovějších (zejména bezpečnostních) aktualizací operačního systému
- Nastavení parametrů TCP/IP na všech aktivních síťových adaptérech
- Funkčnost všech síťových připojení — jak do lokální sítě, tak do Internetu (vhodným nástrojem je např. příkaz `ping`, který zjišťuje dobu odezvy počítače zadaného jménem nebo IP adresou).

Tyto testy vám ušetří mnoho komplikací při pozdějším odstraňování případných problémů.

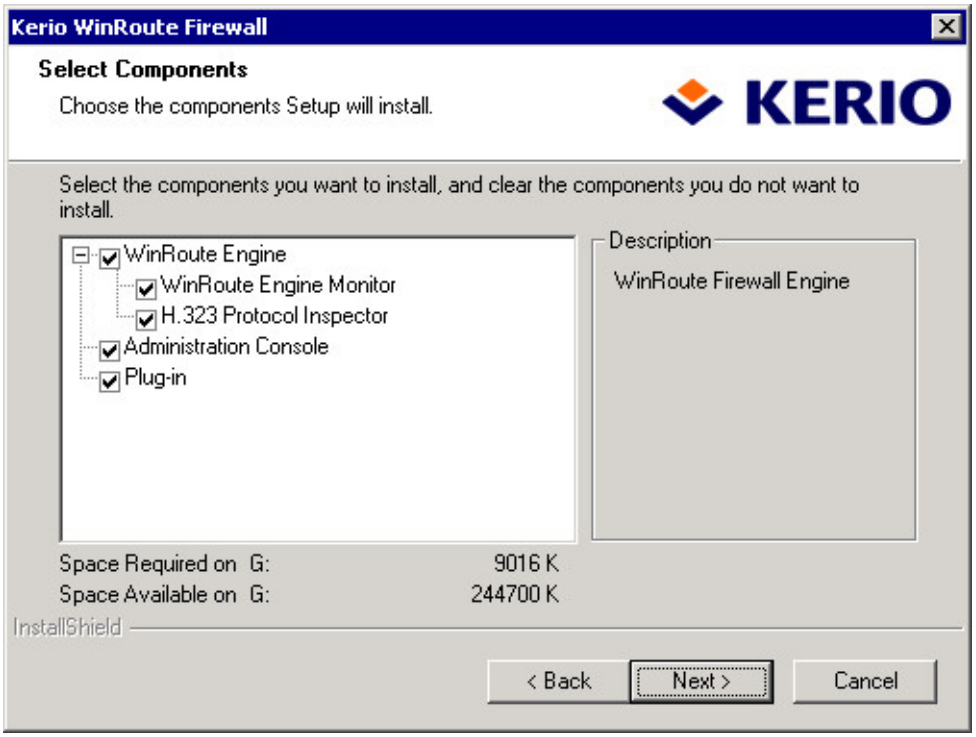
Poznámka: Všechny podporované operační systémy obsahují ve standardní instalaci všechny komponenty, které *WinRoute* pro svoji činnost vyžaduje.

Postup instalace a počáteční konfigurace

Po spuštění instalačního programu (např. `kerio-kwf-5.0.4-win.exe`) se zobrazí průvodce pro nastavení základních parametrů serveru, případně import některých nastavení z programu *WinRoute Pro 4.x*.

Poznámka: Používáte-li *WinRoute Pro 4.x* a budete chtít importovat nastavení, zastavte před instalací *WinRoute* službu *WinRoute Firewall Engine* (aby se změny nastavení uložily do systémového registru). V žádném případě však neprovádějte deinstalaci *WinRoute Pro 4.x* — došlo by ke ztrátě všech nastavení!

Prvním krokem je výběr typu instalace — *Typical* (plná), *Compact* (minimální, tj. bez nápovědy) nebo *Custom* (vlastní). Instalace typu *Custom* umožňuje výběr volitelných komponent programu:



- *WinRoute Firewall Engine* — vlastní výkonné jádro aplikace
- *WinRoute Engine Monitor* — utilita pro ovládání *WinRoute Firewall Engine* a sledování jeho stavu (ikonka na liště)
- *H.323 Protocol Inspector* — inspekční modul protokolové sady H.323 (protokoly IP telefonie — např. hlasová komunikace programem *Microsoft NetMeeting*)
- *Kerio Administration Console* — program *Kerio Administration Console* (univerzální konzola pro správu serverových aplikací firmy Kerio Technologies)
- *Plug-in* — modul *Kerio Administration Console* pro správu *WinRoute*

Podrobný popis komponent *WinRoute* naleznete v kapitole 2.4.

Poznámka: Je-li typ instalace *Custom*, pak se instalační program chová takto:

- všechny označené komponenty se instalují nebo aktualizují
- všechny neoznačené komponenty se neinstalují nebo odstraní

Při instalaci nové verze *WinRoute* přes stávající (upgrade) je tedy třeba označit všechny komponenty, které mají zůstat zachovány.

Po výběru volitelných komponent následuje vlastní instalace (tj. zkopírování souborů na pevný disk a nezbytná systémová nastavení). Poté je automaticky spuštěn průvodce nastavením základních parametrů *WinRoute* (viz kapitola 2.8).

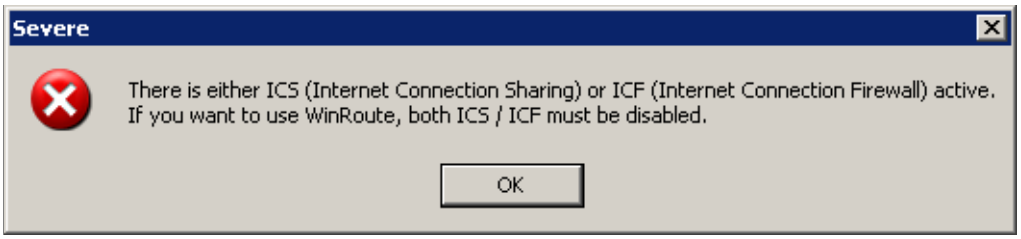
Po instalaci je třeba počítač restartovat (aby mohl být zaveden nízkoúrovňový ovladač *WinRoute*). Po novém startu systému se automaticky spustí *WinRoute Firewall Engine* (běží jako služba anebo, v případě Windows 98 a Me, jako aplikace na pozadí), tj. vlastní výkonné jádro programu, a po přihlášení uživatele také *WinRoute Engine Monitor*.

Kolizní systémové služby

Instalační program *WinRoute* detekuje, zda nejsou spuštěny systémové služby, které by mohly způsobovat kolize se službou *WinRoute Firewall Engine*.

1. *Internet Connection Sharing* a *Internet Connection Firewall*

   Je-li na některém rozhraní počítače, kam má být *WinRoute* nainstalován, zapnuto *Sdílení internetového připojení* (*Internet Connection Sharing* — Windows Me, 2000 nebo XP), případně *Internet Connection Firewall* (Windows XP), zobrazí se toto varovné hlášení:

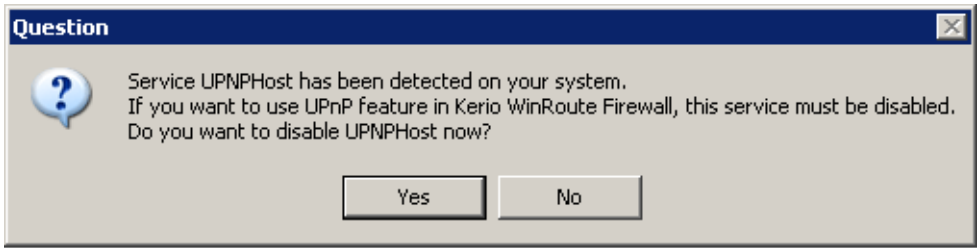
   

   Před stisknutím tlačítka *OK* vypněte obě tyto služby na všech rozhraních, kde jsou zapnuty. Při nesplnění této podmínky nebude *WinRoute* fungovat správně!

2. *Universal Plug and Play Device Host* a *SSDP Discovery Service*

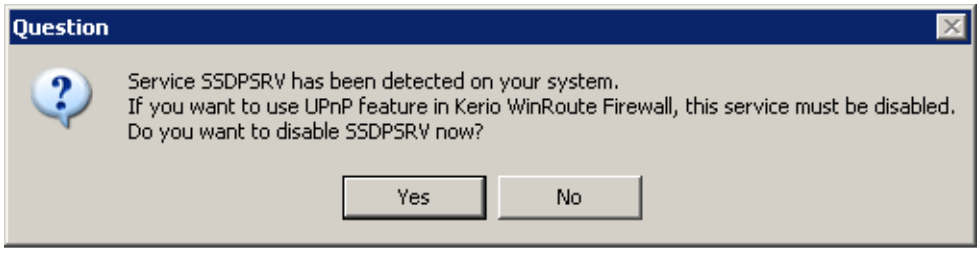
   Tyto dvě služby tvoří podporu protokolu *UPnP* (Universal Plug and Play) v operačním systému Windows XP. Chcete-li používat službu *UPnP* ve *WinRoute* (viz kapitola 10.5), musejí být obě tyto služby vypnuty, aby nedošlo ke kolizi portů.

- Je-li detekována služba *Universal Plug and Play Device Host*, zobrazí se tento dialog:



  Stisknutím tlačítka *Ano* (*Yes*) bude služba *Universal Plug and Play Device Host* zastavena a zakázáno její automatické spouštění při startu systému. Tlačítko *Ne* (*No*) ponechá stav a parametry této služby beze změn.

- Je-li detekována služba *SSDP Discovery Service*, zobrazí se tento dialog:



  Význam obou tlačítek je stejný jako v předchozím případě.

Poznámka: Podrobnosti o *UPnP* naleznete v kapitole 10.5.

2.4 Komponenty WinRoute

WinRoute sestává z následujících tří částí:

WinRoute Firewall Engine Vlastní výkonný program, který realizuje všechny služby a funkce. Běží jako služba (ve Windows NT 4.0, 2000 a XP) nebo jako skrytá aplikace (ve Windows 98 a Me).

WinRoute Engine Monitor Slouží k monitorování a změně stavu *Engine* (zastaven / spuštěn), nastavení spouštěcích preferencí (tj. zda se má *Engine* a/nebo *Monitor* sám spouštět automaticky při startu systému) a snadnému spuštění administrační konzole. Podrobnosti naleznete v kapitole 2.5.

Poznámka: WinRoute Firewall Engine je zcela nezávislý na aplikaci *WinRoute Engine Monitor*. *Engine* tedy může běžet, i když se na liště nezobrazuje ikona (běží jako služba, příp. ve Windows 98/Me jako skrytá aplikace).

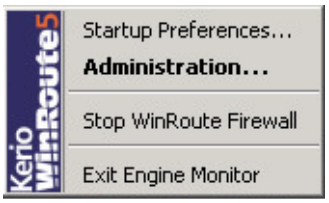
Kerio Administration Console Univerzální program pro lokální či vzdálenou správu produktů firmy Kerio Technologies. Pro připojení k určité aplikaci je třeba modul obsahující specifické rozhraní pro tuto aplikaci. Při instalaci *WinRoute* je *Kerio Administration Console* nainstalována s příslušným modulem (tzv. *plug-in*). Použití *Kerio Administration Console* pro správu *WinRoute* je podrobně popsáno v kapitole 3.

2.5 WinRoute Engine Monitor

WinRoute Engine Monitor je utilita, která slouží k ovládání a monitorování stavu *WinRoute Firewall Engine*. Tato komponenta se zobrazuje jako ikona na hlavním panelu.

Je-li *WinRoute Firewall Engine* zastaven, objeví se přes ikonu červený kruh s bílým křížkem. Spouštění či zastavování *WinRoute Firewall Engine* může za různých okolností trvat až několik sekund. Na tuto dobu ikona zešedne a je neaktivní, tzn. nereaguje na myš.

Dvojitým kliknutím levým tlačítkem na tuto ikonu lze spustit program *Kerio Administration Console* (viz dále). Po kliknutí pravým tlačítkem se zobrazí menu, v němž je možné zvolit následující funkce:



Startup Preferences Volby pro automatické spouštění *WinRoute Firewall Engine* a *WinRoute Engine Monitoru* při startu systému. Výchozí nastavení (po instalaci) je obě volby zapnuty.

WinRoute Administration Tato volba spouští program *Kerio Administration Console* (totéž lze provést dvojitým kliknutím levým tlačítkem na ikonu *WinRoute Engine Monitoru*)

Start / Stop WinRoute Firewall Engine Spuštění nebo zastavení *WinRoute Firewall Engine* (text se mění v závislosti na jeho stavu).

Exit Ukončení programu *WinRoute Engine Monitor*. Tato volba nezastavuje *WinRoute Firewall Engine*, na což je uživatel upozorněn varovným hlášením.

Poznámka: Pokud má licence *WinRoute* omezenou platnost (např. neregistrovaná zkušební verze), pak se 7 dní před vypršením licence automaticky zobrazí informace o tom, že se blíží konec její platnosti. Zobrazení této informace se pak periodicky opakuje až do okamžiku, kdy licence vyprší.

2.6 Upgrade a deinstalace

Tato kapitola popisuje upgrade *WinRoute* v rámci verze `5` (např. z verze `5.0.0` na verzi `5.1.0`). Postup přechodu z verze `4.x` na verzi `5.x` je popsán v kapitole 2.3.

Chcete-li provést upgrade (tj. instalovat novější verzi získanou např. z WWW stránek výrobce), stačí jednoduše spustit instalaci nové verze. Instalační program dokáže automaticky zastavit všechny komponenty *WinRoute*, pokud běží. Při instalaci je rozpoznán adresář, kde je stávající verze nainstalována, a nahrazeny příslušné soubory novými. Přitom zůstanou zachována veškerá nastavení i soubory záznamů.

Upozornění: V případě upgrade se nedoporučuje měnit nabízený instalační adresář!

Pro deinstalaci je vhodné zastavit všechny tři komponenty *WinRoute*. Program lze deinstalovat průvodcem *Přidat nebo odebrat programy* v *Ovládacích panelech*. Při deinstalaci mohou být volitelně smazány také všechny soubory v adresáři `WinRoute Firewall`.

2.7 Zálohování a přenos konfigurace

Veškeré konfigurační informace *WinRoute* jsou uloženy v adresáři, kde je *WinRoute* nainstalován. Jedná se o tyto soubory:

winroute.cfg Hlavní konfigurační soubor

users.cfg Informace o uživatelských účtech a skupinách

logs.cfg Konfigurace záznamů

host.cfg Parametry týkající se počítače, na němž je *WinRoute* nainstalován. Tento soubor není nutné zálohovat.

ids.cfg Rezervováno pro budoucí použití

Údaje v těchto souborech jsou uloženy ve formátu XML v kódování UTF-8. Zkušený uživatel je tedy může poměrně snadno ručně modifikovat, případně automaticky generovat vlastní aplikací. Zálohu či přenos konfigurace lze provést pouhým zkopírováním těchto souborů.

Upozornění

Před jakoukoliv manipulací s konfiguračními soubory je doporučeno zastavit *WinRoute Firewall Engine*. Konfigurační soubory jsou totiž načítány pouze při jeho spuštění. Ukládány jsou při provedení jakékoliv změny v konfiguraci a při zastavení *Engine*. Změny, které byly v konfiguračních souborech provedeny za běhu *Engine*, budou při jeho zastavení přepsány konfigurací v operační paměti.

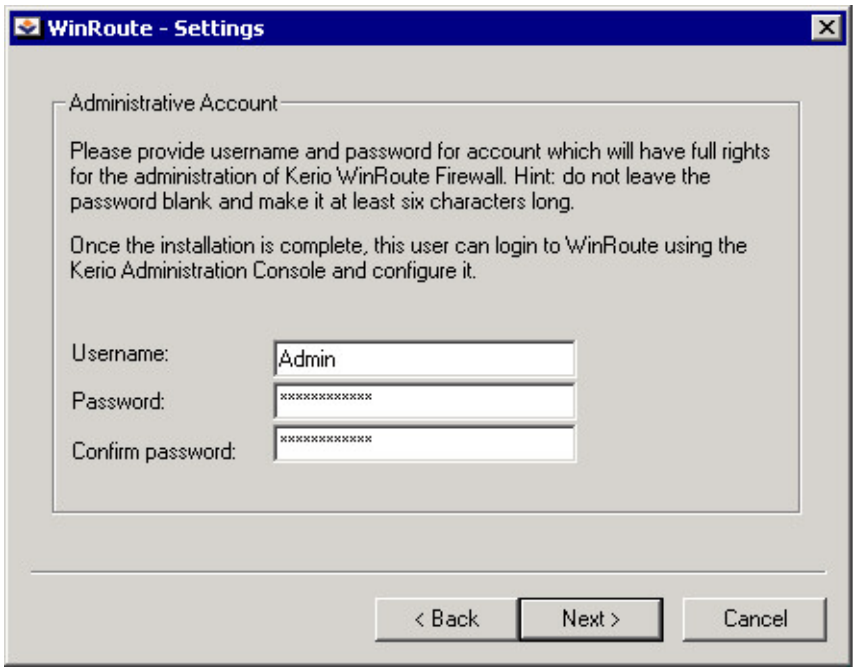
2.8 Průvodce počáteční konfigurací

Instalační program automaticky spouští průvodce, který vám pomůže nastavit základní parametry *WinRoute*.

Poznámka: Konfigurační průvodce je k dispozici pouze v anglickém jazyce.

Nastavení administrátorského hesla

Velmi důležitým krokem pro zajištění bezpečnosti vašeho firewallu je nastavení administrátorského hesla. Ponecháte-li prázdné heslo, pak se vystavujete riziku, že se ke konfiguraci *WinRoute* přihlásí nepovolaná osoba.



V dialogu pro nastavení účtu je třeba zadat heslo (*Password*) a zopakovat jej pro kontrolu (*Confirm Password*). V položce *Username* můžete změnit jméno administrátora (standardně `Admin`).

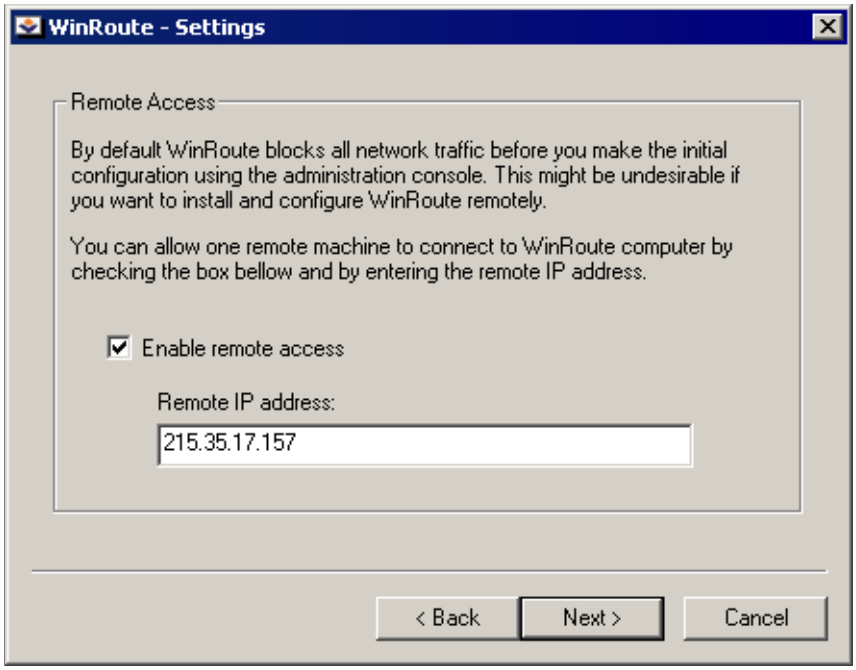
Poznámka: Pokud je *Kerio WinRoute Firewall* nainstalován jako upgrade *WinRoute Pro 4.x*, pak je tento krok přeskočen — administrátorský účet bude rovněž importován z *WinRoute Pro 4.x* (viz dále).

Vzdálený přístup

Bezprostředně po prvním spuštění *WinRoute Firewall Engine* dojde k blokování veškeré síťové komunikace (požadovaná komunikace pak musí být povolena vytvořením pravidel — viz kapitola 5). Je-li *WinRoute* instalován vzdáleně (např. pomocí terminálového přístupu), pak se v tomto okamžiku přeruší také komunikace se vzdáleným klientem (a konfigurace *WinRoute* musí být provedena lokálně).

Pro umožnění vzdálené instalace a správy lze ve druhém kroku průvodce počáteční konfigurací zadat IP adresu počítače, odkud bude po spuštění *WinRoute Firewall Engine* možné pracovat s firewallem vzdáleně (např. pomocí terminálových služeb). *WinRoute* povolí veškerou komunikaci mezi firewallem a vzdáleným počítačem.

Poznámka: Pokud *WinRoute* instalujete lokálně, pak tento krok přeskočte. Povolení plného přístupu ze vzdáleného počítače může představovat bezpečnostní hrozbu.



Enable remote access Tato volba povoluje plný přístup k počítači s *WinRoute* z jedné vybrané IP adresy.

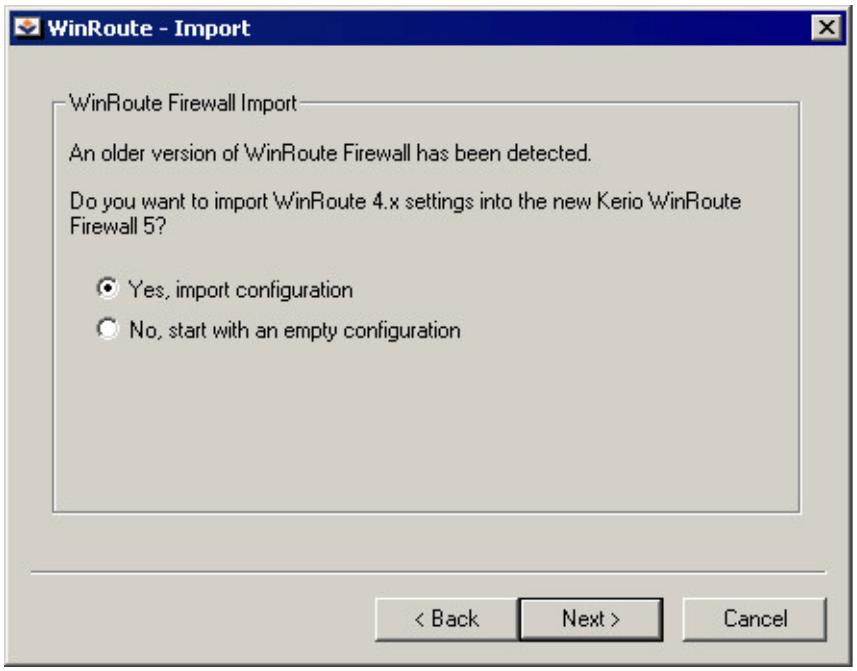
Remote IP address IP adresa počítače, odkud se vzdáleně připojujete (např. terminálovým klientem). Do této položky lze uvést pouze jeden počítač, který musí být zadán IP adresou (nikoliv DNS jménem).

Upozornění: Po nastavení *WinRoute* průvodcem komunikačními pravidly (viz kapitola 5.1) se pravidlo pro povolení vzdáleného přístupu zruší.

Import nastavení z WinRoute Pro 4.x

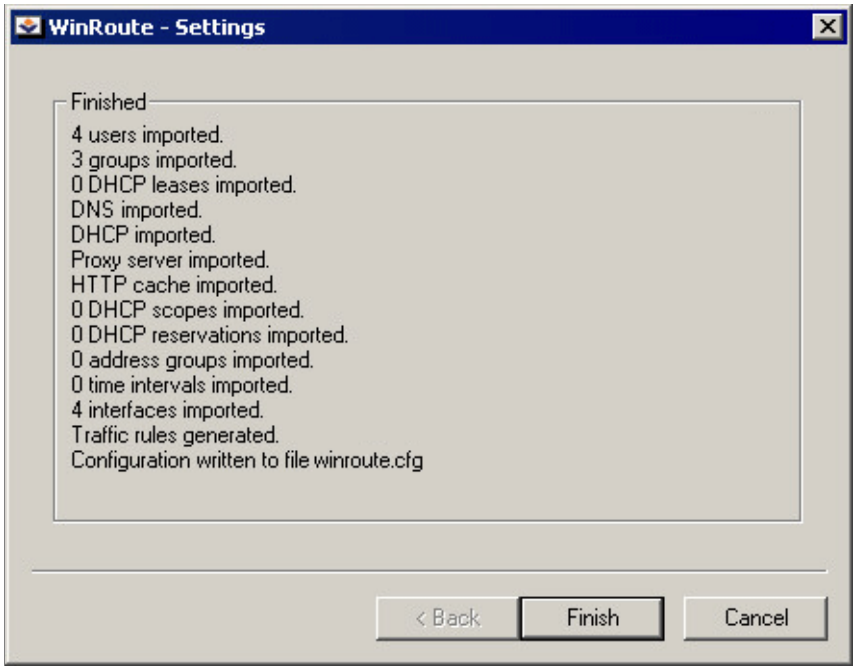
Je-li na počítači, kde byl instalační program spuštěn, detekována instalace *WinRoute Pro 4.x*, konfigurační průvodce nabídne import nastavení z tohoto programu.

Upozornění: Před instalací aplikace *Kerio WinRoute Firewall* je třeba *WinRoute Pro 4.x* zastavit (na to vás instalační program rovněž upozorní). V žádném případě však nesmí být odinstalován — tím by došlo ke ztrátě všech nastavení!



Volba *Yes, import configuration* znamená, že konfigurace má být importována; volba *No, start with an empty configuration* import neprovede. V každém případě se však nastavení *WinRoute Pro 4.x* zálohuje, aby byl možný návrat k předchozí verzi. Záloha se ukládá do podaresáře `OldCfg`.

Po importu konfigurace budete informováni o jeho výsledku (počtu importovaných položek konfigurace).



Po stisknutí tlačítka *Finish* se ukončí konfigurační průvodce a dokončí vlastní instalace *WinRoute*.

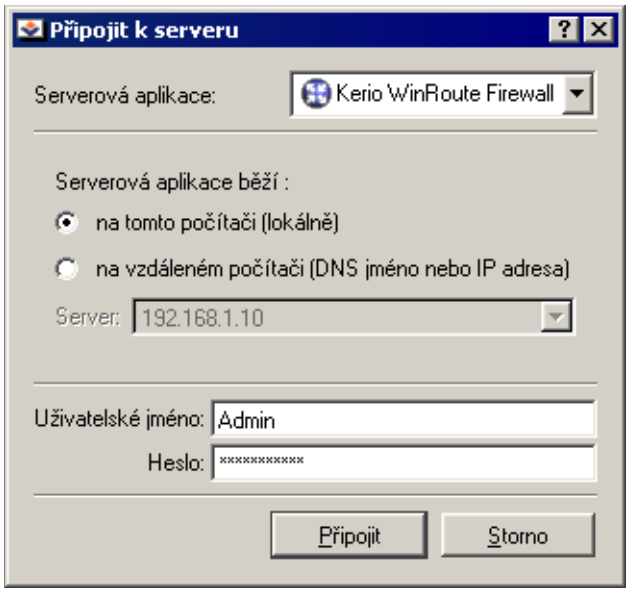
Kapitola 3

Administrační program

Program *Kerio Administration Console* slouží ke správě produktů firmy *Kerio Technologies* včetně firewallu *WinRoute*. *Kerio Administration Console* umožňuje lokální správu (tj. z téhož počítače, na kterém *WinRoute Firewall Engine* běží) i vzdálenou správu (z libovolného jiného počítače). Komunikace mezi *Kerio Administration Console* a *WinRoute Firewall Engine* je šifrována, což zabraňuje jejímu odposlechu a zneužití.

3.1 Lokální administrace

Spusťte program *Kerio Administration Console* (z programové skupiny *Kerio* nebo z kontextového menu utility *WinRoute Engine Monitor*). Po stisknutí tlačítka *Připojit* v nástrojovém panelu (nebo volbou *Akce / Připojit*) se zobrazí dialog pro přihlášení.



Nejprve je třeba vybrat typ serverové aplikace, která má být spravována — v tomto případě *Kerio WinRoute Firewall*.

Zvolte *na tomto počítači (lokálně)*. *Kerio Administration Console* se připojí k serveru běžícímu na tomtéž počítači (`localhost`). Zadejte příslušné uživatelské jméno a heslo (při prvním přihlášení použijte administrátorský účet vytvořený při instalaci). Tlačítkem *Připojit* se připojte. Po úspěšném přihlášení se v *Kerio Administration Console* otevře okno pro správu *WinRoute Firewall Engine*.

Poznámka: Při prvním přihlášení po instalaci *WinRoute* se nejprve automaticky spustí průvodce vytvořením komunikačních pravidel, který slouží k počáteční konfiguraci *WinRoute*. Podrobný popis tohoto průvodce najdete v kapitole 5.1.

3.2 Vzdálená administrace

Na počítači, odkud se budete vzdáleně připojovat, je třeba nainstalovat program *Kerio Administration Console* s modulem pro správu *WinRoute*. Spusťte instalační program *WinRoute* a zvolte instalaci *Administration Console*.

Spusťte program *Kerio Administration Console* a v přihlašovacím dialogu zvolte, že *WinRoute Firewall Engine* běží *na vzdáleném počítači (DNS jméno nebo IP adresa)*. Do pole *Server* vyplňte DNS jméno počítače, na němž *WinRoute Firewall Engine* běží (např. `fw.firma.cz`) nebo odpovídající IP adresu (např. `192.168.1.1`). Zadejte příslušné uživatelské jméno a heslo a tlačítkem *Připojit* se připojte.

3.3 Proč se nelze přihlásit?

Jestliže se při pokusu o přihlášení objeví okno se zprávou *Připojení k serverové aplikaci selhalo*, jedná se zřejmě o některou z následujících příčin:

- Chybné uživatelské jméno nebo heslo. Ujistěte se, že jméno a heslo zadáváte správně. Mějte na paměti, že v hesle se rozlišují malá a velká písmena. Přesvědčte se, že nedošlo k nechtěnému přepnutí klávesy *Caps Lock* nebo přepnutí klávesnice do jiné jazykové verze.

- Uživatel nemá práva pro správu *WinRoute*. Pomocí *Kerio Administration Console* se může přihlásit pouze uživatel, který má umožněn přístup ke správě *WinRoute Firewall Engine*. Detaily najdete v kapitole 9.1.

- Na počítači, na který se chcete přihlásit, neběží *WinRoute Firewall Engine*. Ten je třeba nejprve spustit (pomocí utility *WinRoute Engine Monitor* nebo v panelu *Služby* ve Windows NT 4.0 / 2000 / XP).

- Vzdálená administrace není povolena nebo je povolena pouze z určité skupiny IP adres. Detaily najdete v kapitole 10.1.

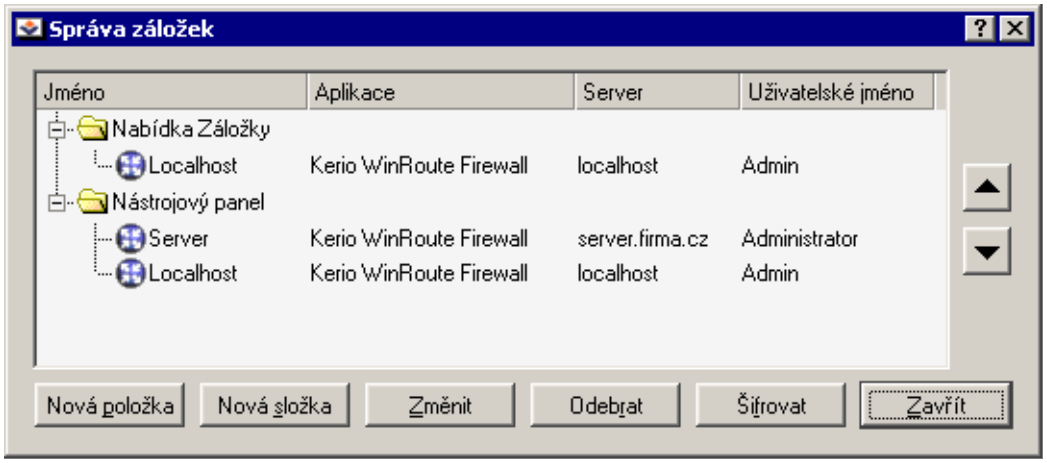
3.4 Záložky

Záložek lze využít, připojujete-li se pomocí *Kerio Administration Console* často střídavě k různým serverovým aplikacím (např. spravujete *WinRoute* na několika různých místech současně). *Kerio Administration Console* umožňuje uložit si parametry jednotlivých připojení (IP adresy, uživatelská jména, případně i hesla) a připojovat se komfortně pouhým výběrem položky z nabídky nebo stisknutím tlačítka v nástrojovém panelu.

Definice a uspořádání záložek

Záložky lze vytvářet a následně třídit do složek a mazat v nabídce

Záložky / Správa záložek.



V levé části okna jsou zobrazeny dva stromy záložek: *Nabídka Záložky* (menu *Záložky*) a *Nástrojový panel* (tlačítka na nástrojové liště). Nástrojová lišta se standardně zobrazuje v horní části okna vedle tlačítek

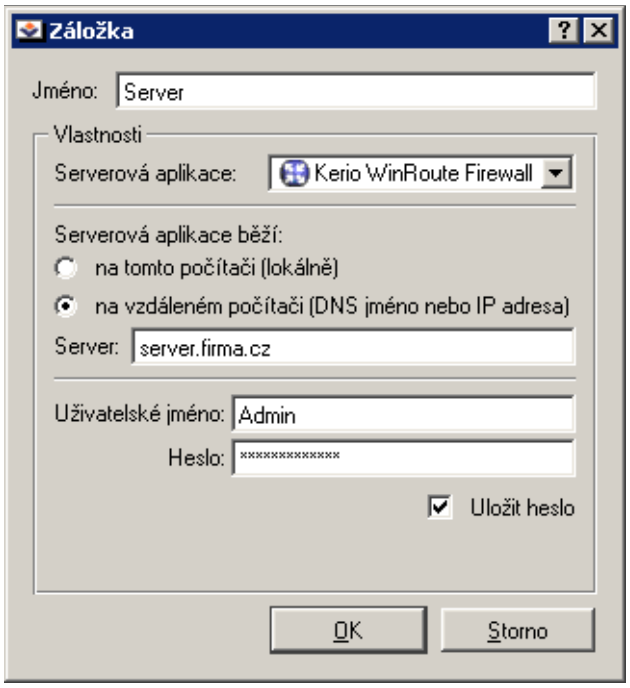
Připojit a *Odpojit*, lze ji však přemístit, a to i mimo hlavní okno *Kerio Administration Console*.

Tlačítky v dolní části okna lze záložky vytvářet a upravovat, příp. mazat:

Nová položka Dialog pro vytvoření nové záložky.

Položka *Jméno* slouží k pojmenování záložky — pod tímto názvem pak bude zobrazována v nabídce *Záložky* či na nástrojové liště.

Volba *Uložit heslo* určuje, zda má být heslo uloženo do souboru záložek společně s ostatními informacemi. Pokud ano, záložku lze použít na jedno kliknutí, v opačném případě je třeba při každém použití záložky zadat heslo znovu. Pro bezpečné



uložení přihlašovacích údajů *Kerio Administration Console* umožňuje celý soubor záložek zašifrovat a ochránit heslem — viz dále.

Ostatní položky tohoto dialogu jsou shodné se standardním přihlašovacím dialogem (tj. je třeba specifikovat typ serverové aplikace a počítač, na němž běží, uživatelské jméno a heslo pro přístup ke správě). Podrobnosti najdete v kapitole 3.1, resp. 3.2.

Nová složka Vytvoření nové složky (pouze ve stromu *Nabídka záložek*)

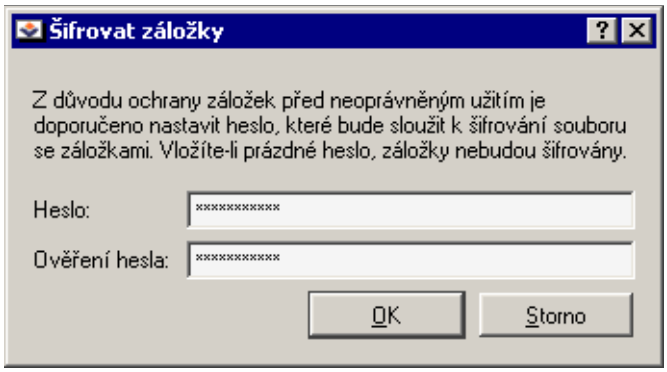
Šifrovat Zašifrování souboru záložek a nastavení hesla pro jeho použití. Při dalším spuštění *Kerio Administration Console* je uživatel vyzván, aby zadal heslo k souboru záložek.

Upozornění: Heslo může obsahovat pouze tisknutelné znaky (písmena, číslice, interpunkční znaménka). V hesle se rozlišují malá a velká písmena.

Při každém dalším spuštění *Kerio Administration Console* se zobrazí dialog pro zadání hesla k souboru se záložkami. Zadá-li uživatel nesprávné heslo nebo tento dialog stornuje, může *Kerio Administration Console* používat, ale záložky nebudou k dispozici.

Zavřít Ukončení dialogu *Správa záložek*

TIP: Pro účelné využití záložek je vhodné hesla pro jednotlivá připojení ukládat, aby umožňovaly skutečně rychlé připojení. Vždy ale soubor záložek tlačítkem *Šifrovat* zašifrujte a nastavte heslo pro jeho použití, aby nemohl být zneužit neoprávněnou osobou.



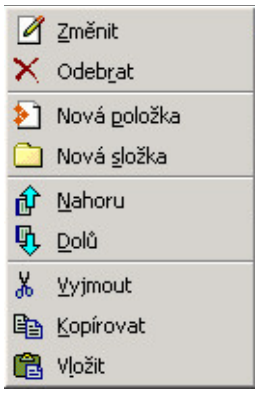
Kontextové menu pro záložky

Stisknutím pravého tlačítka na vybrané záložce se zobrazí kontextové menu, které obsahuje funkce *Změnit* a *Odebrat* (úprava, resp. smazání vybrané záložky),

Nová položka a *Nová složka* (viz výše) a *Nahoru* a *Dolů* (přesun vybrané záložky v rámci složky

Nabídka Záložky nebo *Nástrojový panel*). Dále jsou zde standardní funkce

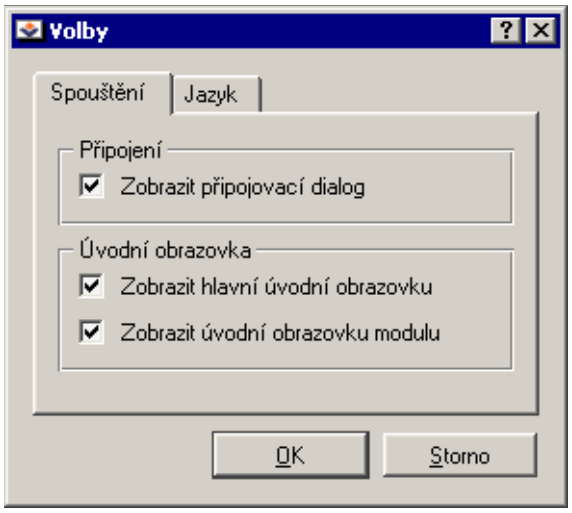
Vyjmout, *Kopírovat* a *Vložit*, kterými lze např. přesunout záložky z jedné složky do druhé.



3.5 Spouštěcí preference a jazyk

Spouštěcí preference a jazyk je možné nastavit v nabídce *Nastavení / Volby*.

Volby v záložce *Spouštění* určují, jak se má *Kerio Administration Console* chovat po spuštění, resp. přihlášení k serverové aplikaci:

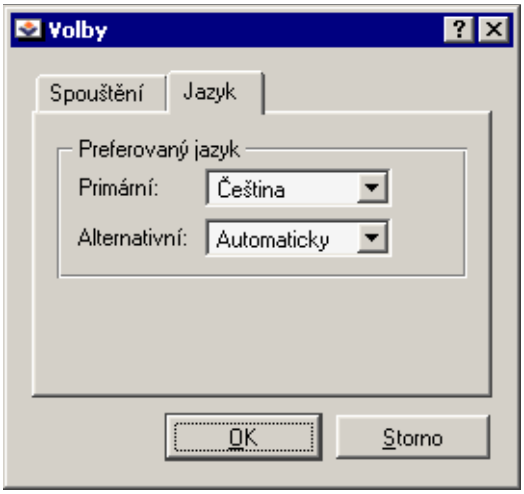


Zobrazit připojovací dialog Automatické otevření přihlašovacího dialogu při každém spuštění *Kerio Administration Console* (jako po stisknutí tlačítka *Připojit*, resp. volbě *Akce / Připojit*).

Zobrazit hlavní úvodní obrazovku Zobrazení úvodní obrazovky *Kerio Administration Console* při jejím startu

Zobrazit úvodní obrazovku modulu Zobrazení úvodní obrazovky modulu (serverové aplikace — např. *WinRoute*) po přihlášení.

Záložka *Jazyk* slouží k nastavení primárního a alternativního jazyka *Kerio Administration Console*.



Tato nastavení určují pořadí, v jakém se bude *Kerio Administration Console* pokoušet nalézt definiční soubory jednotlivých jazyků (`*.qm`). Nebude-li nalezen definiční soubor

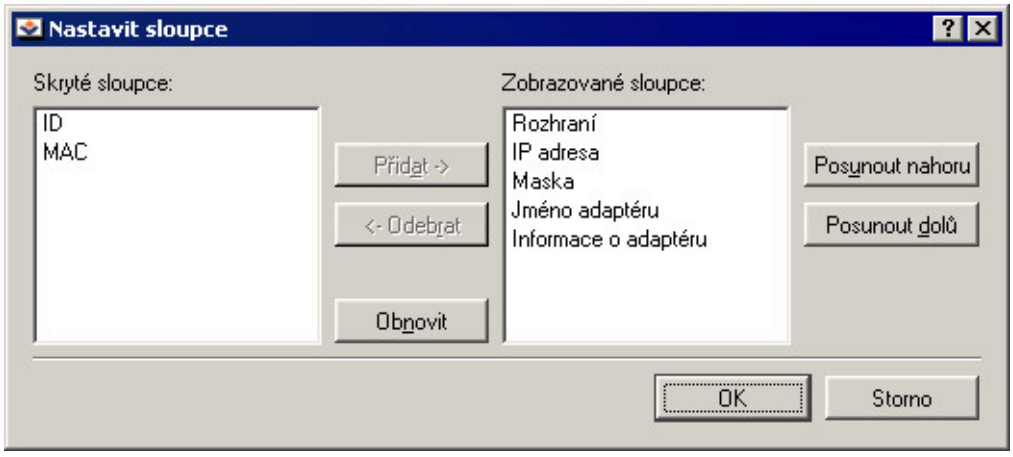
pro primární jazyk, zkusí se sekundární. Pokud nebude nalezen ani ten, nastaví se výchozí jazyk — angličtina.

Volba *Automaticky* nastavuje jazyk podle nastavení země a jazyka v operačním systému (je-li k dispozici příslušný definiční soubor).

3.6 Nastavení pohledů

V mnoha sekcích *Kerio Administration Console* má zobrazení tvar tabulky, přičemž každý řádek obsahuje jeden záznam (např. údaje o jednom uživateli, jednom rozhraní apod.) a sloupce obsahují jednotlivé položky tohoto záznamu (např. jméno rozhraní, název adaptéru, hardwarovou adresu, IP adresu atd.).

Správce *WinRoute* má možnost upravit si způsob zobrazení informací v jednotlivých sekcích dle vlastní potřeby či vkusu. V každé z jmenovaných sekcí se po stisknutí pravého tlačítka myši zobrazí kontextová nabídka obsahující volbu *Nastavit sloupce*. Tato volba otevírá dialog, v němž je možné nastavit, které sloupce mají být zobrazeny a které mají zůstat skryty.



Pole *Skryté sloupce* obsahuje sloupce, které zůstanou skryty, a pole *Zobrazované sloupce* ty, které mají být zobrazeny. Tlačítkem *Přidat* se vybraný sloupec ze skupiny skrytých přesune do zobrazovaných, tlačítkem *Odebrat* naopak. Tlačítko *Obnovit* uvede nastavení sloupců do výchozího stavu.

Tlačítka *Posunout nahoru* a *Posunout dolů* slouží k posunu vybraného sloupce ve skupině nahoru nebo dolů. Tím můžete určit pořadí, v jakém mají být sloupce zobrazeny.

Pořadí sloupců lze také upravit v pohledu samotném: klikněte levým tlačítkem myši na název sloupce, podržte jej a přesuňte na požadované místo.

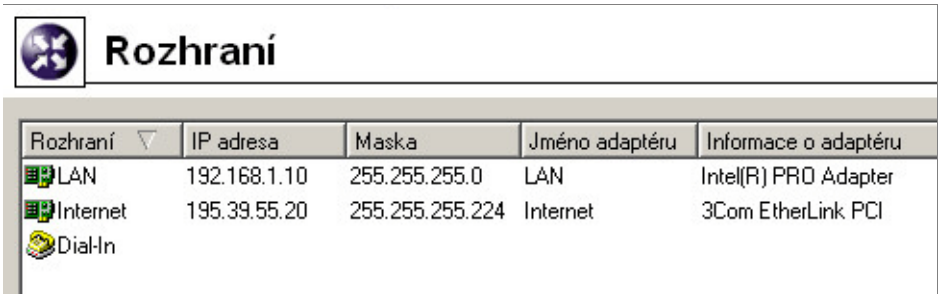
Šířku jednotlivých sloupců lze upravit posunutím dělicí čáry mezi záhlavími sloupců.

Kapitola 4

Nastavení rozhraní a síťových služeb

4.1 Rozhraní

WinRoute pracuje jako směrovač nad všemi síťovými rozhraními, která jsou v systému instalována. V administračním programu se rozhraní zobrazují v sekci *Konfigurace / Rozhraní*.



Rozhraní Název, který identifikuje rozhraní v rámci *WinRoute*. Zvolte jej tak, aby bylo zcela jednoznačné, o který adaptér se jedná (např. *Internet* pro rozhraní vedoucí do Internetu). Doporučujeme vyhnout se duplicitním názvům rozhraní (způsobily by komplikace při definici komunikačních pravidel či úpravách směrovací tabulky).

Název rozhraní může být kdykoliv později změněn (viz dále), aniž by tím došlo k ovlivnění funkce *WinRoute*.

Ikonka vlevo od názvu zobrazuje typ rozhraní (adaptér nebo vytáčené připojení).

Poznámka: Nebyl-li dosud název rozhraní zadán ručně, obsahuje tato položka jméno adaptéru z operačního systému (viz položka *Jméno adaptéru*).

Jméno adaptéru Pojmenování adaptéru v operačním systému (např. „Připojení k místní síti 2“). Slouží pro snazší orientaci, o který adaptér se jedná.

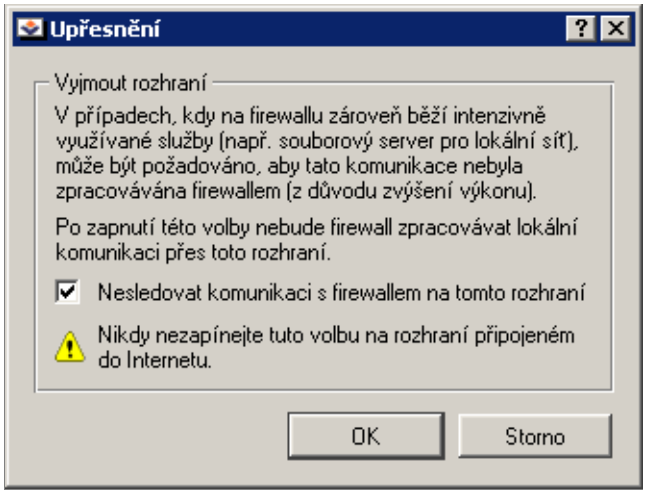
Informace o adaptéru Identifikační řetězec adaptéru, který vrací příslušný ovladač zařízení.

IP adresa, Maska IP adresa a maska subsítě přiřazené tomuto rozhraní.

Tlačítka pod seznamem rozhraní umožňují provádět určité akce s vybraným rozhraním. Není-li vybráno žádné rozhraní, nebo vybrané rozhraní danou funkci nepodporuje, jsou příslušná tlačítka neaktivní.

Přidat Tímto tlačítkem lze přidat novou vytáčenou linku. Pokud byl přidán nový síťový adaptér, je třeba jej nainstalovat a nakonfigurovat v operačním systému. *WinRoute* jej pak detekuje automaticky.

Změnit Zobrazení detailních informací a úprava parametrů vybraného rozhraní. Tlačítko *Upřesnění* zobrazuje dialog, ve kterém může být zakázáno sledování komunikace s firewallem na daném rozhraní.



Odebrat Odstranění vybraného rozhraní z *WinRoute*. Odstranit rozhraní můžete pouze za následujících podmínek:

- jedná se o vytáčenou linku, která je momentálně zavěšena
- jedná se o síťový adaptér, který již není v systému fyzicky přítomen nebo není aktivní

Aktivní síťový adaptér či vytočenou linku *WinRoute* nepovolí odebrat.

Poznámka: Záznam o již neexistujícím síťovém adaptéru nemá negativní vliv na chod *WinRoute* — je považován za neaktivní, stejně jako vytáčená linka v zavěšeném stavu.

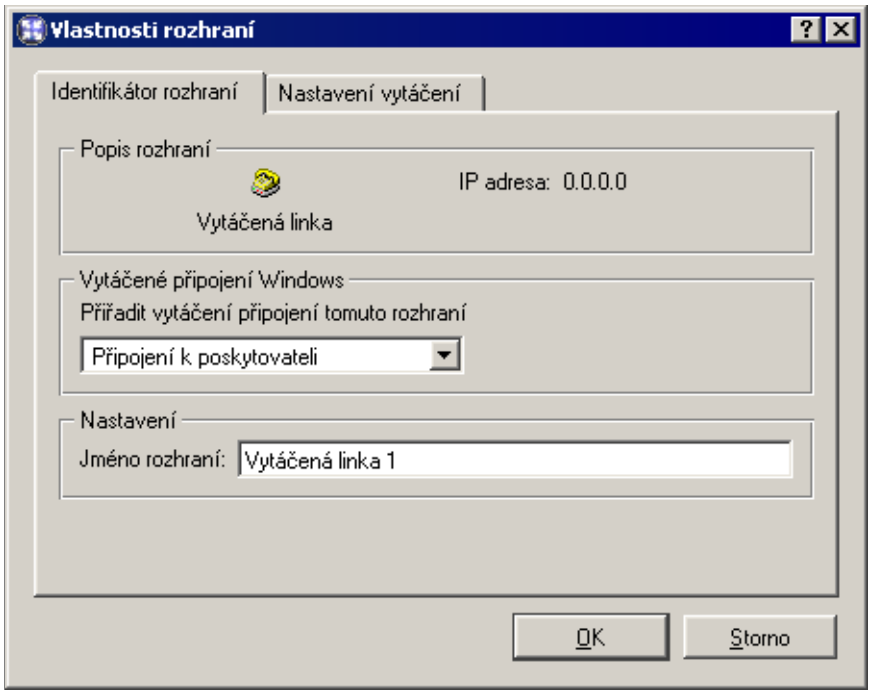
Vytočit, Zavěsit Ruční ovládání vybrané linky. Vytáčet a zavěšovat linky lze také pomocí WWW administračního rozhraní (viz kapitola 7). Je-li vybrán síťový adaptér, jsou tato tlačítka neaktivní.

Obnovit Tlačítkem lze aktualizovat seznam rozhraní.

Přidání nebo změna rozhraní

Po stisknutí tlačítka *Přidat* nebo *Změnit* se otevře dialog pro definici či změnu parametrů vybraného rozhraní.

Poznámka: Následující popis se zabývá vytáčenými linkami. V případě síťového adaptéru lze nastavit jediný parametr — *Jméno rozhraní*.



Přiřadit vytáčené připojení... V tomto poli vyberte položku telefonického připojení Windows (RAS), kterou používáte pro připojení k vašemu poskytovateli Internetu.

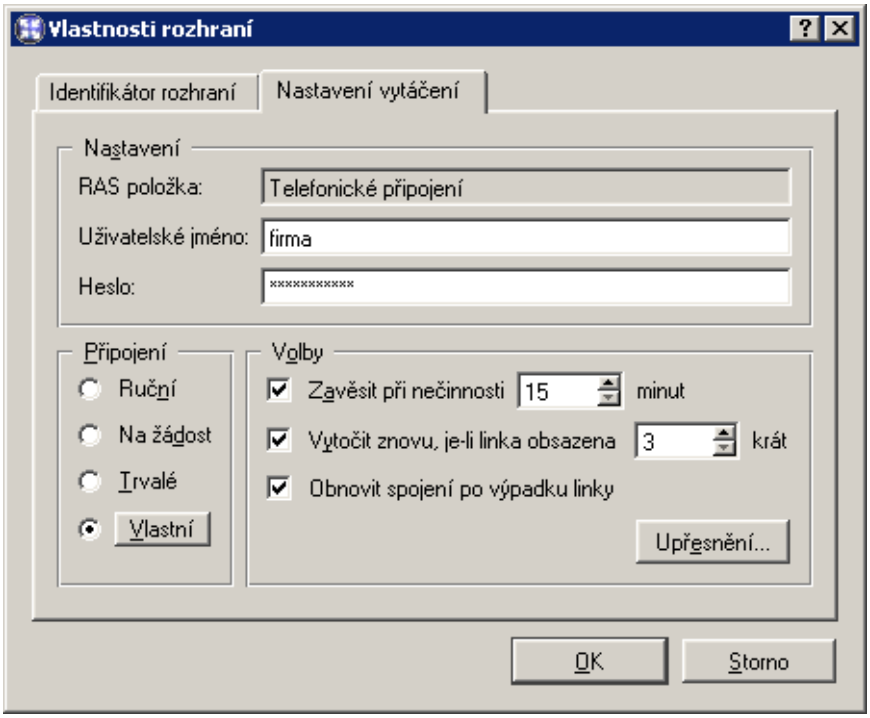
Poznámka: Doporučujeme vytvořit toto připojení a otestovat jeho funkčnost ještě před instalací *WinRoute*.

Jméno rozhraní Jednoznačné jméno, které bude vytvořenou linku identifikovat v rámci *WinRoute*.

Záložka *Nastavení vytáčení* slouží k podrobnému nastavení, kdy a jakým způsobem bude linka vytáčena. Výchozí nastavení je ruční vytáčení.

RAS položka Položka *Telefonického připojení* Windows, která byla vybrána v záložce *Identifikátor rozhraní*. Název RAS položky se zde zobrazuje pro lepší přehlednosti.

Uživatelské jméno, Heslo Přihlašovací jméno a příslušné heslo pro toto připojení. Tyto údaje je třeba zadat, aby je měl *WinRoute* k dispozici (ve Windows jsou uloženy v profilu konkrétního uživatele, odkud je služba *WinRoute Firewall Engine* nemůže načíst).

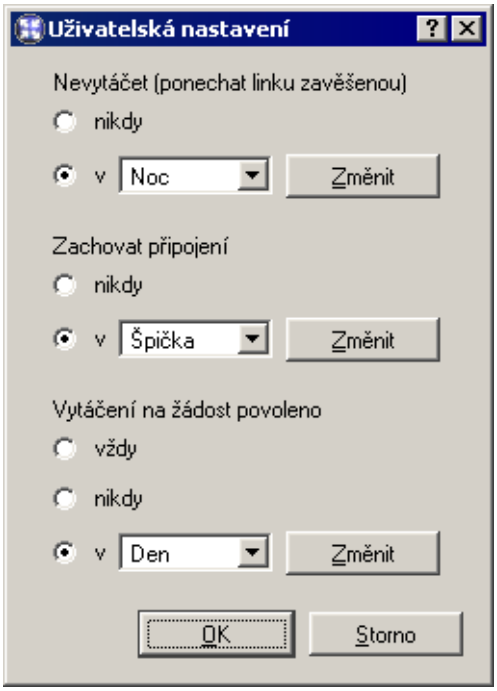


Připojení Způsob, jakým bude linka vytáčena:

- *Ruční* — linku bude možné vytočit pouze ručně (v programu *Kerio Administration Console* nebo prostřednictvím WWW administračního rozhraní — viz kapitola 7)
- *Na žádost* — linka bude automaticky vytáčena na základě příchozího požadavku (paketu z lokální sítě směrovaného do Internetu). Konfigurace *WinRoute* a operačního systému pro správnou funkci vytáčení na žádost je podrobně popsána v kapitole 10.3.
- *Trvalé* — linka bude vytočena okamžitě při startu služby *WinRoute Firewall Engine* a bude v tomto stavu udržována (tzn. např. po výpadku či ručním zavěšení se linka automaticky ihned znovu vytočí)
- *Vlastní* — tato volba umožňuje detailní nastavení časů, kdy má být povoleno vytáčení na žádost a kdy má být linka trvale připojena nebo trvale zavěšena.

  V jednotlivých sekcích dialogového okna je možné vybrat časový interval, v němž má příslušná akce platit. Tlačítko *Změnit* otevírá dialog pro definici časových intervalů, kde můžete interval upravit nebo vytvořit nový. Detailní informace o časových intervalech naleznete v kapitole 8.2.

  Uživatelské nastavení vytáčení funguje následovně:



- Nejvyšší prioritu má volba *Nevytáčet*. Je-li aktuální čas v tomto intervalu, linka zůstane zavěšena (nebo se ihned zavěsí, pokud je vytočena).
- Dále se testuje interval pro volbu *Zachovat připojení*. Po dobu trvání tohoto intervalu bude linka udržována v připojeném stavu.
- Jako poslední se testuje volba *Vytáčení na žádost povoleno*. Je-li nastavena na *vždy*, bude vytáčení na žádost povoleno kdykoliv mimo interval uvedený u volby *Nevytáčet*.

Volby Upřesňující parametry vytáčení pro typy *Ruční*, *Na žádost* a *Vlastní*. V případě trvalého připojení tyto volby nemají význam (*WinRoute* se stále snaží udržovat linku ve vytočeném stavu).

Zavěsit při nečinnosti Doba, po které dojde k automatickému zavěšení, jestliže přes rozhraní neprocházejí žádná data. S každým procházejícím paketem je časovač doby nečinnosti nulován.

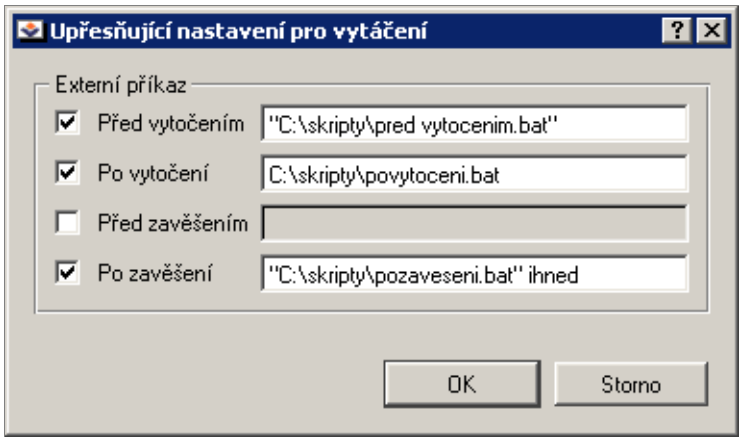
Optimální dobu je nejlépe určit experimentálně. Příliš krátké časy způsobí časté vytáčení linky, naopak příliš dlouhé budou udržovat linku vytočenou po dlouhou dobu — obojí má za následek zvýšení celkových nákladů na internetové připojení.

Vytočit znovu, je-li linka obsazena Je-li při pokusu o vytočení linka obsazena, bude *WinRoute* opakovat vytáčení, dokud se připojení nezdaří nebo do zadaného maximál-

ního počtu pokusů. Nepodaří-li se linku připojit, bude požadavek vytočení ignorován (tzn. vytočení nemůže být automaticky přeplánováno na pozdější dobu).

Obnovit spojení po výpadku linky Jestliže byl detekován výpadek linky, *WinRoute* bude automaticky zkoušet vytočit připojení znovu.

Upřesnění Dialog poskytuje možnost spustit jakoukoli aplikaci nebo příkaz operačního systému při těchto akcích: *Před vytočením*, *Po vytočení*, *Před zavěšením* a *Po zavěšení*.



Cesta k souboru musí být vždy kompletní. Pokud cesta obsahuje mezeru, musí být vložena do uvozovek, jinak bude část za mezerou považována za parametr. Text je považován za parametr, pokud je oddělen mezerou nebo pokud je cesta k souboru označena uvozovkami.

Pokud je zadán příkaz do prvního a/nebo třetího řádku (*Před vytočením*, *Před zavěšením*), po spuštění programu se nečeká na jeho ukončení.

Upozornění:

Pokud je*WinRoute* spuštěn v operačním systému jako služba, aplikace bude spuštěna pouze na pozadí.

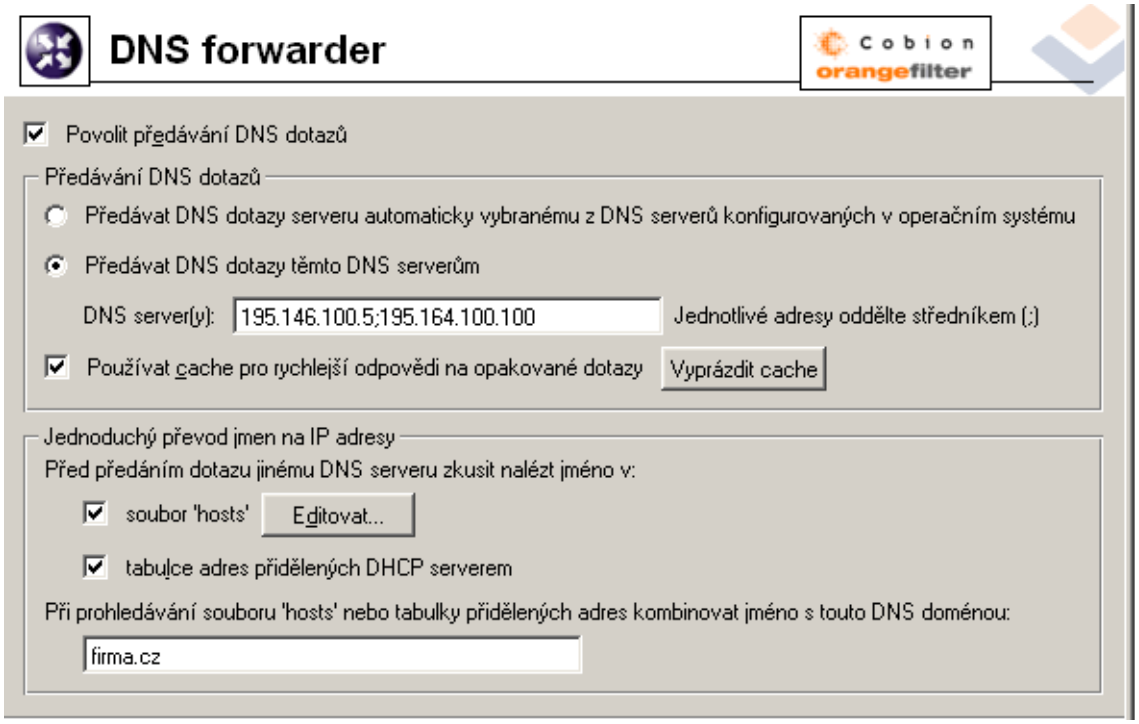
4.2 DNS forwarder

Modul *DNS Forwarder* slouží ve *WinRoute* ke zjednodušení konfigurace DNS na počítačích v lokální síti a pro zrychlení odpovědí na opakované DNS dotazy. DNS na lokálních počítačích můžete obecně nastavit jedním z následujících způsobů:

- použít IP adresu primárního, příp. i záložního DNS serveru Vašeho poskytovatele Internetu. Toto řešení je regulérní, avšak odezvy na DNS dotazy budou značně pomalé.

- použít DNS server v lokální síti (je-li k dispozici). Tento DNS server musí mít přístup do Internetu, aby dokázal odpovídat i na dotazy mimo lokální doménu.
- použít *DNS Forwarder* ve *WinRoute*. Ten může rovněž sloužit jako jednoduchý DNS server pro lokální doménu (viz dále) či jako forwarder pro váš stávající DNS server.

Ve výchozím nastavení *WinRoute* je *DNS Forwarder* zapnut a nastaven pro předávání DNS dotazů na jeden z DNS serverů konfigurovaných v operačním systému (typicky DNS server přidělený poskytovatelem internetového připojení). Podrobnou konfiguraci lze provést v sekci *Konfigurace / DNS Forwarder*.



Povolit předávání DNS dotazů Tato volba zapíná / vypíná modul *DNS Forwarder* (služba používá protokol UDP a běží na portu 53). Pokud ve vaší síťové konfiguraci *DNS Forwarder* nepoužijete, můžete jej vypnout. Chcete-li na tomtéž počítači provozovat jiný DNS server, pak jej *musíte* vypnout — jinak by nastala kolize na uvedeném portu.

Předávání DNS dotazů *DNS Forwarder* musí znát alespoň jeden DNS server, na který bude dotazy předávat. Tato volba určuje, jakým způsobem získá IP adresu tohoto serveru:

- *Předávat DNS dotazy serveru automaticky vybranému...* — předpokládá se, že počítač s *WinRoute* má funkční připojení do Internetu. Součástí nutné konfigurace

TCP/IP je také nastavení jednoho nebo více DNS serverů (ve Windows se DNS servery nastavují na konkrétním adaptéru, mají však globální platnost v rámci celého operačního systému).

DNS Forwarder může přečíst toto nastavení a používat stejné DNS servery. Jednoznačnou výhodou této volby je, že počítače v lokální síti budou vždy používat tentýž DNS server jako počítač s *WinRoute* — tím lze předejít mnoha problémům.

- *Předávat dotazy těmto DNS serverům* — DNS dotazy budou předávány na zadané DNS servery (je-li zadáno více serverů, považují se za primární, sekundární atd.). Tuto volbu použijte, chcete-li mít kontrolu nad tím, kam jsou DNS dotazy předávány, nebo pokud potřebujete vytvořit složitější konfiguraci.

Používat cache pro rychlejší odpovědi Zapnutím této volby budou odpovědi na všechny dotazy ukládány do lokální vyrovnávací paměti (cache) *DNS Forwarderu*. Odpovědi na opakované dotazy tak budou mnohonásobně rychlejší (opakovaným dotazem je i stejný dotaz vyslaný různými klienty).

Poznámky:

1. Doba uchování DNS záznamů v cache je specifikována přímo v každém záznamu (zpravidla 1 den).

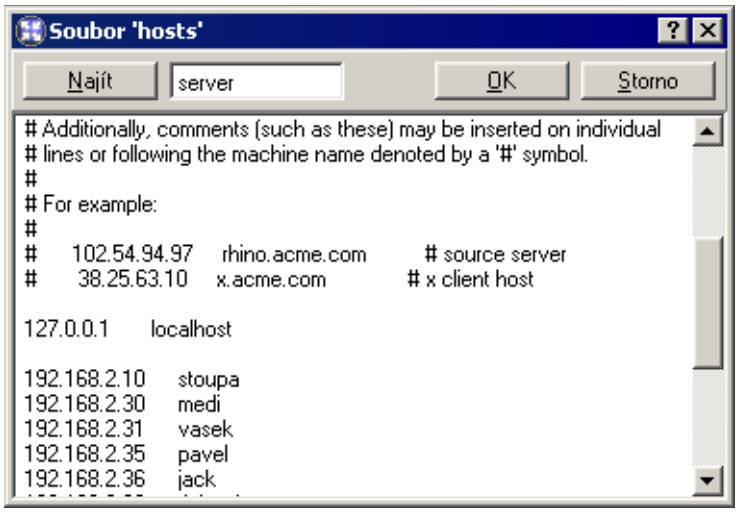
2. Použití DNS cache zrychlí také činnost HTTP proxy serveru (viz kapitola 4.4).

Vyprázdnit cache Stisknutím tohoto tlačítka dojde ke smazání všech záznamů ve vyrovnávací paměti *DNS Forwarderu* (bez ohledu na jejich dobu životnosti). Tuto funkci lze využít např. při změně konfigurace, při testování vytáčení na žádost, odhalování chyb apod.

Jednoduchý převod jmen na IP adresy *DNS Forwarder* může zároveň fungovat jako jednoduchý DNS server pro jednu vaši lokální doménu. K tomuto účelu využívá:

- *systémový soubor 'hosts'* — tento soubor se nalézá v každém operačním systému, který podporuje TCP/IP. Každý řádek tohoto souboru obsahuje IP adresu počítače a seznam odpovídajících DNS jmen. Při každém DNS dotazu je nejprve prohledáván tento soubor, zda se v něm nachází požadované jméno (případně IP adresa), a teprve pak (není-li nalezeno) se dotaz předává DNS serveru.

  Stejným způsobem se chová *DNS Forwarder*, je-li tato volba zapnuta. Tlačítko *Editovat* otevírá speciální editor, kterým lze soubor `hosts` upravovat přímo v *Kerio Administration Console*, a to i v případě, kdy je k *WinRoute* připojena vzdáleně (tj. z jiného počítače).



- *tabulku adres přidělených DHCP serverem* — jsou-li počítače v lokální síti konfigurovány pomocí DHCP serveru ve *WinRoute* (viz kapitola 4.3), pak má DHCP server informace o tom, jaká IP adresa byla přiřazena kterému počítači. Počítač při startu systému vysílá požadavek na přidělení IP adresy, který obsahuje i jméno počítače.

  DNS Forwarder má přístup do tabulek DHCP serveru a může tedy zjistit, jaká IP adresa je v tomto okamžiku přidělena danému jménu počítače. Na dotaz na jméno počítače v lokální síti tedy vždy odpoví správnou (aktuální) IP adresou.

Kombinovat jméno ... s touto doménou Do tohoto pole zadejte jméno lokální DNS domény.

Jestliže počítač vysílá požadavek na přidělení IP adresy, vkládá do něj pouze své jméno (doménu v tomto okamžiku ještě nezná). Aby *DNS Forwarder* dokázal správně zodpovídat dotazy na plně kvalifikovaná lokální DNS jména (tj. jména včetně domény), musí znát jméno lokální domény.

Pro snazší pochopení uveďme jednoduchý příklad:

Lokální doména má jméno `firma.cz`. V lokální síti je počítač se jménem `honza` nastavený pro automatickou konfiguraci IP adresy z DHCP serveru. Po startu operačního systému vyšle tento počítač DHCP požadavek obsahující jméno stanice `honza`. DHCP server mu přidělí IP adresu `192.168.1.56`. Ve své tabulce uchová informaci o tom, že tato IP adresa byla přidělena stanici se jménem `honza`.

Jiný počítač, který bude chtít s tímto počítačem komunikovat, vyšle dotaz na jméno `honza.firma.cz` (jedná se o počítač `honza` v doméně `firma.cz`). Kdyby *DNS Forwarder* neznal jméno lokální domény, přeposlal by tento dotaz na konfigurovaný DNS server, protože by nerozpoznal, že se jedná o jméno v lokální doméně. Takto však může lokální doménu `firma.cz` oddělit a jméno `honza` s příslušnou IP adresou nalezne v tabulce DHCP serveru.

Poznámka: Je-li v *DNS Forwarderu* zadána lokální doména, pak mohou být v souboru `HOSTS` uvedena lokální jména včetně domény nebo bez ní — v obou případech budou dotazy zodpovídány správně.

4.3 DHCP server

DHCP server (*Dynamic Host Configuration Protocol*) slouží ke snadné konfiguraci TCP/IP na počítačích v síti. Klientská stanice vyšle při startu operačního systému požadavek na konfiguraci, který je zachycen DHCP serverem. DHCP server vybere vhodné konfigurační parametry (tj. IP adresu s příslušnou maskou subsítě a další volitelné parametry — např. adresu výchozí brány, adresy DNS serverů, jméno domény apod.) a přidělí je klientské stanici. Veškeré parametry pro klienty se nastavují pouze centrálně na serveru — na jednotlivých stanicích stačí nastavit volbu, aby byly parametry TCP/IP konfigurovány automaticky z DHCP serveru. Toto je ve většině operačních systémů (např. Windows, Linux atd.) výchozí volba — na klientských stanicích pak není třeba nic nastavovat.

DHCP server přiděluje klientům IP adresy z definovaného rozsahu, a to zpravidla na určitou dobu (tzv. dobu pronájmu, angl. *lease time*). Před uplynutím této doby musí klient požádat o prodloužení pronájmu, jinak bude po této době IP adresa považována za volnou a v případě nedostatku volných adres ji DHCP server přidělí jinému klientovi. Vše probíhá automaticky a pro uživatele zcela transparentně.

V DHCP serveru mohou být rovněž definovány tzv. rezervace — tj. určitým klientům budou vždy přidělovány dané IP adresy. Adresa může být rezervována pro hardwarovou (MAC) adresu nebo jméno počítače. Tito klienti pak mají pevné IP adresy, které jsou konfigurovány automaticky.

Mezi hlavní výhody použití DHCP serveru patří výrazně nižší náročnost administrace (vše stačí nastavit pouze na serveru, není třeba konfigurovat jednotlivé stanice) a eliminace mnoha potenciálních chyb (např. přidělení téže IP adresy dvěma různým stanicím, chybné nastavení výchozí brány na některé stanici apod.).

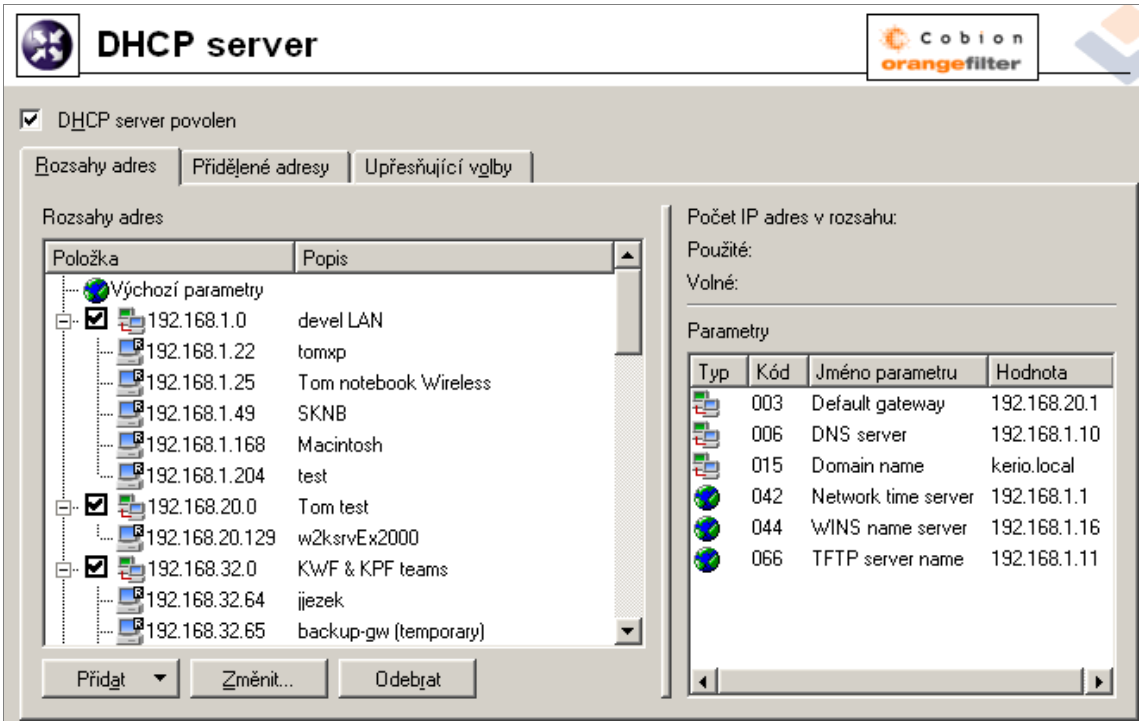
Konfigurace DHCP serveru

K nastavení DHCP serveru ve *WinRoute* slouží sekce *Konfigurace / DHCP server*. Zde lze definovat rozsahy IP adres, rezervace, volitelné parametry a zobrazovat informace o přidělených adresách a statistiky DHCP serveru.

DHCP server se zapíná a vypíná volbou *DHCP server povolen* v horní části okna. Konfiguraci je možné provádět i v případě, že je DHCP server vypnut.

Definice rozsahů IP adres

K definici rozsahů IP adres včetně volitelných parametrů slouží záložka *Rozsahy adres*. Záložka je rozdělena na dvě části, z nichž první obsahuje rozsahy adres a rezervace:

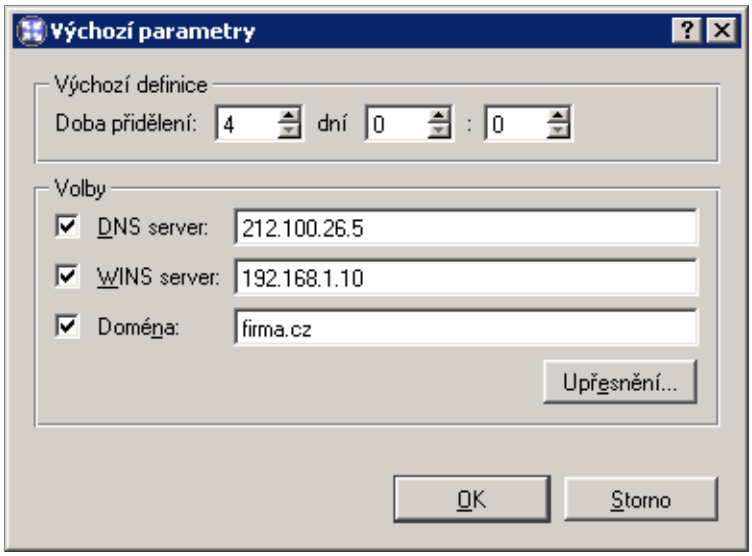


Ve sloupci *Položka* se zobrazují subsítě, v nichž jsou rozsahy IP adres definovány. Zaškrtávací pole vedle adresy subsítě slouží k aktivaci či deaktivaci daného rozsahu adres (takto lze rozsah dočasně „vyřadit“, aniž by bylo nutné jej odstraňovat a poté znovu přidávat). Pod každou subsítí jsou pak zobrazovány rezervace IP adres, které jsou v ní definovány.

První položkou v tabulce jsou *Výchozí parametry*, kde lze nastavit výchozí parametry pro DHCP server.

Doba přidělení Doba, na kterou je IP adresa klientům přidělována. Pokud během této doby klient nepožádá o prodloužení pronájmu nebo o uvolnění adresy, pak je po jejím uplynutí tato adresa automaticky uvolněna a může být přidělena jinému klientovi.

DNS server Může být uveden libovolný DNS server (případně více DNS serverů oddělených středníky). Jako primární DNS server (tj. na prvním místě) však doporučujeme uvádět *DNS Forwarder* ve *WinRoute* (tj. IP adresu počítače s *WinRoute*). *DNS Forwarder* totiž dokáže spolupracovat s DHCP serverem (viz kapitola 4.2) a na dotazy na jména lokálních počítačů bude vždy odpovídat správnou IP adresou.



WINS server IP adresa WINS serveru.

Doména Lokální internetová doména. Pokud lokální doména neexistuje, pak tento parametr nenastavujte.

Upřesnění Tlačítko *Upřesnění* otevírá dialog s kompletním výčtem volitelných parametrů, které protokol DHCP podporuje (včetně výše uvedených). V tomto dialogu je možné přidat libovolný parametr, který DHCP server podporuje, a nastavit jeho hodnotu.

Výchozí parametry jsou přidělovány automaticky rozsahům adres, pokud není změněna konfigurace konkrétního rozsahu adres (dialog *Rozsah IP adres / Volby*). Podobně funguje vztah mezi rozsahem adres a rezervacemi (pokud nezměníte parametry přímo u konkrétní rezervace, platí parametry nastavené v daném rozsahu adres). Platnost parametrů je tedy podřízena hierarchii stromové struktury, do které jsou rozsahy řazeny.

Volbou *Přidat / Rozsah adres* se zobrazí dialog pro definici rozsahu adres.

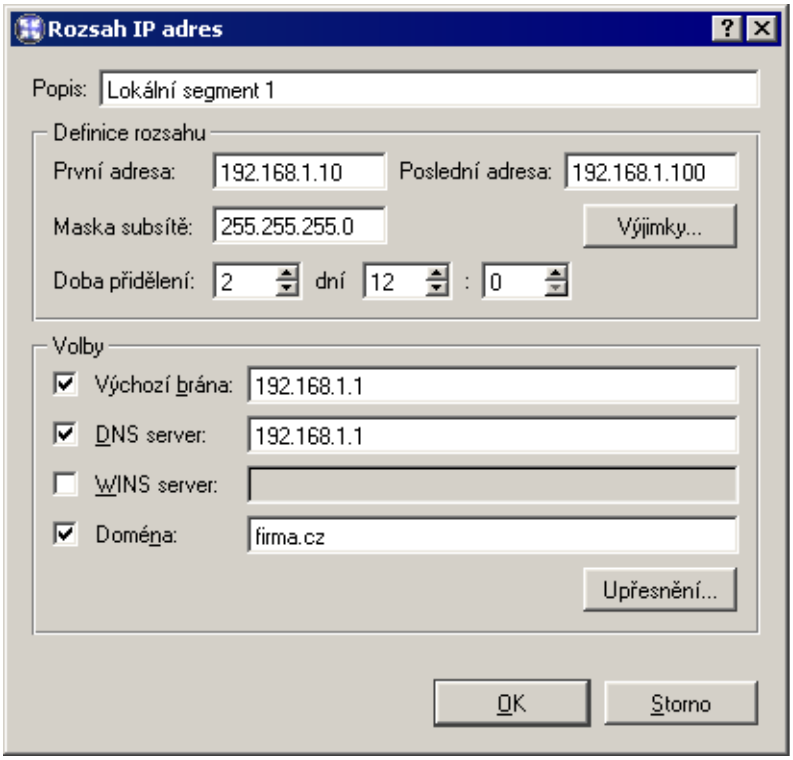
Poznámka: V každé subsíti je možné definovat pouze jeden rozsah adres.

Popis Textový popis vytvářeného rozsahu adres (pro přehled správce *WinRoute*).

První adresa, Poslední adresa Počáteční a koncová adresa definovaného rozsahu.

Poznámka: Doporučujeme definovat větší rozsah IP adres, než je skutečný počet počítačů v dané subsíti.

Maska subsítě Maska odpovídající subsíti, v níž je tento rozsah adres definován. Maska subsítě je přidělována klientům společně s IP adresou.



Poznámka: Program *Kerio Administration Console* kontroluje, zda počáteční a koncová adresa rozsahu patří do téže subsítě vymezené zadanou maskou. Pokud není tato podmínka splněna, bude po stisknutí tlačítka *OK* hlášena chyba.

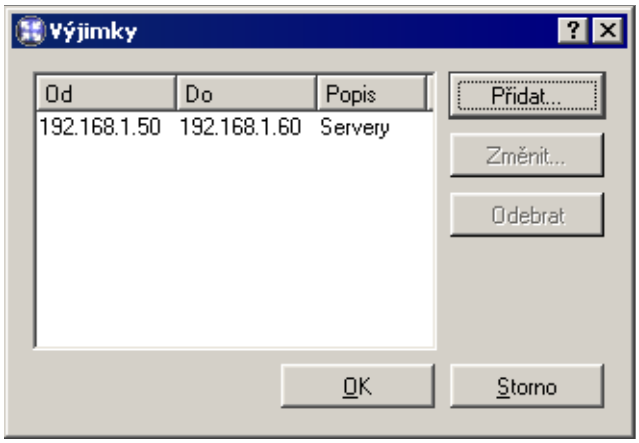
Doba přidělení Doba, na kterou je IP adresa klientům přidělována. Pokud během této doby klient nepožádá o prodloužení pronájmu nebo o uvolnění adresy, pak je po jejím uplynutí tato adresa automaticky uvolněna a může být přidělena jinému klientovi.

Výjimky *WinRoute* umožňuje definovat v každé subsíti pouze jeden rozsah IP adres. Chceme-li vytvořit několik nesouvislých rozsahů, provedeme to následovně:

- vytvoříme rozsah adres pokrývající všechny požadované rozsahy
- definujeme tzv. výjimky — tj. rozsahy adres, které nemají být přidělovány

Příklad: V subsíti `192.168.1.0` chceme vytvořit dva rozsahy adres: `192.168.1.10` až `192.168.1.49` a `192.168.1.61` až `192.168.1.100`. Adresy `192.168.1.50` až `192.168.1.60` mají zůstat vyhrazeny pro jiné účely.

Vytvoříme rozsah adres `192.168.1.10` až `192.168.1.100` a stisknutím tlačítka *Výjimky* definujeme rozsah adres `192.168.1.50` až `192.168.1.60`, které nemají být DHCP serverem přidělovány.



Parametry Dialog *Rozsah IP adres* umožňuje zadání základních DHCP parametrů, které budou klientům přidělovány:

- *Výchozí brána* — musí být uvedena IP adresa směrovače, který je výchozí branou pro subsíť, z níž jsou IP adresy přidělovány (tzn. IP adresa rozhraní, ke kterému je daná subsíť připojena)! Výchozí brána v jiné subsíti nemá žádný smysl (byla by pro klienty nedosažitelná).

- *DNS server* — může být uveden libovolný DNS server (případně více DNS serverů oddělených středníky). Jako primární DNS server (tj. na prvním místě) však doporučujeme uvádět *DNS Forwarder* ve *WinRoute* (tj. IP adresu počítače s *WinRoute*). *DNS Forwarder* totiž dokáže spolupracovat s DHCP serverem (viz kapitola 4.2) a na dotazy na jména lokálních počítačů bude vždy odpovídat správnou IP adresou.

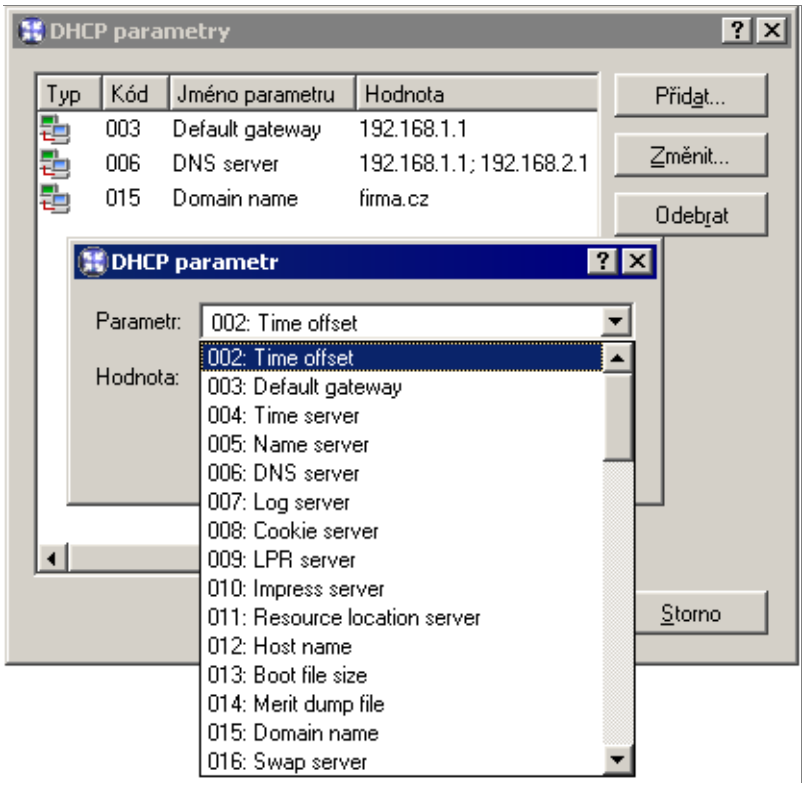
- *WINS server*

- *Doména* — lokální internetová doména. Pokud lokální doména neexistuje, pak tento parametr nenastavujte.

  Upozornění: Tento parametr neslouží k zadání jména Windows NT domény!

Upřesnění... Tlačítko *Upřesnění* otevírá dialog s kompletním výčtem volitelných parametrů, které protokol DHCP podporuje (včetně výše uvedených). V tomto dialogu je možné přidat libovolný parametr, který DHCP server podporuje, a nastavit jeho hodnotu. Dialog je zároveň druhou částí záložky *Rozsah adres*.

Nastavené DHCP parametry a jejich hodnoty pro vybraný rozsah IP adres se zobrazují v pravém sloupci záložky *Rozsahy adres*.



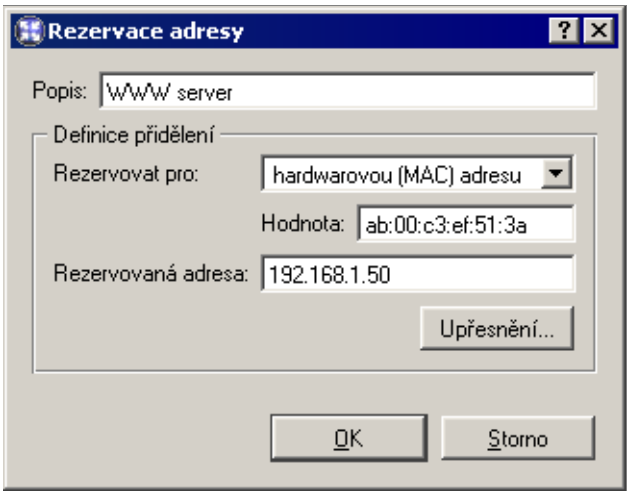
Poznámka: V pravé horní části záložky *Rozsahy adres* jsou zobrazovány jednoduché statistiky DHCP serveru. Pro vybraný rozsah IP adres je uveden:

- celkový počet IP adres v tomto rozsahu
- počet a procentuální podíl přidělených adres
- počet a procentuální podíl volných adres

Počet IP adres v rozsahu:	90
Použité:	46 (52%)
Volné:	44 (48%)

Rezervace IP adresy

DHCP server umožňuje vyhradit (rezervovat) vybranou IP adresu pro konkrétní počítač. Rezervaci vytvoříme v záložce *Rozsahy adres* volbou *Přidat / Rezervaci.*



Rezervovat je možné libovolnou IP adresu, která patří do některé z definovaných subsítí. Nezáleží na tom, zda je tato adresa uvnitř nebo vně rozsahu dynamicky přidělovaných adres, a může být i v některém z rozsahů, které jsou definovány jako výjimky.

IP adresa může být rezervována pro:

- hardwarovou (MAC) adresu počítače — zadává se v podobě hexadecimálních (šestnáctkových) čísel oddělených dvojtečkami — např.:

  ```
  00:bc:a5:f2:1e:50
  ```

  nebo pomlčkami — např.:

  ```
  00-bc-a5-f2-1e-50
  ```

  MAC adresu síťového adaptéru je možné zjistit pomocí nástrojů operačního systému (např. příkaz `ipconfig`), případně speciálního programu dodávaného výrobcem síťového adaptéru.

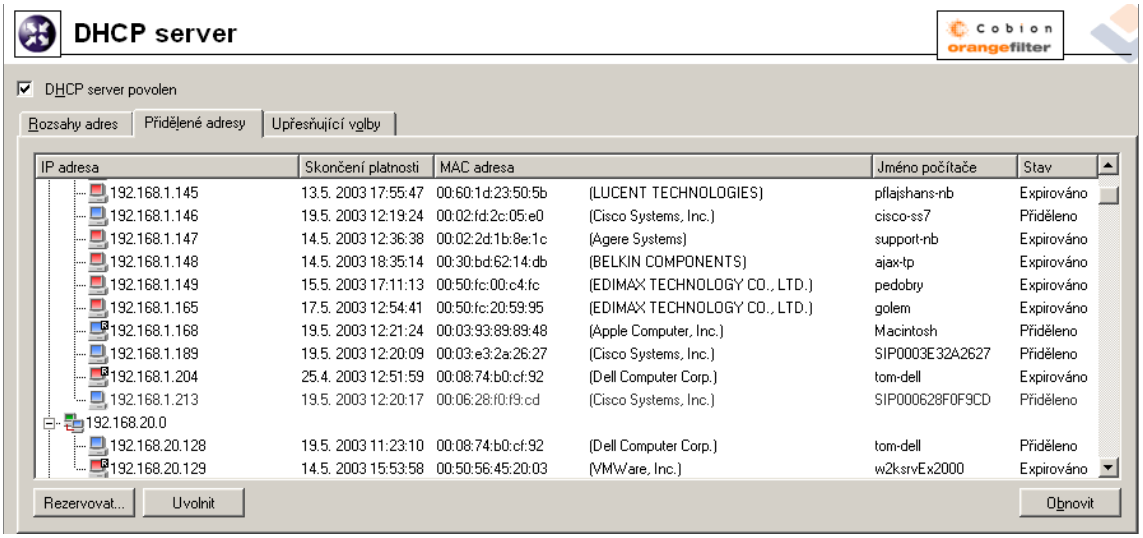
- jméno počítače — většina DHCP klientů posílá v DHCP požadavku jméno počítače (např. všechny operační systémy Windows), příp. je možné klienta nastavit, aby jméno počítače posílal (např. operační systém Linux).

Tlačítko *Upřesnění* otevírá dialog pro nastavení DHCP parametrů, které budou společně s touto adresou přidělovány. Pokud je rezervovaná IP adresa uvnitř již definovaného rozsahu, pak jsou automaticky použity DHCP parametry přiřazené tomuto rozsahu. V dialogu *Rezervace adresy* je možné přidat další parametry, případně nastavit specifické hodnoty již existujících parametrů.

Poznámka: IP adresu lze rezervovat také tak, že v záložce *Přidělené adresy* nalezneme IP adresu, která byla dynamicky přidělena vybranému počítači, a tu pro něj rezervujeme (podrobnosti viz dále).

Přidělené IP adresy

V záložce *Přidělené adresy* se (v podobě stromu) zobrazují rozsahy IP adres a v každém z nich všechny IP adresy, které jsou aktuálně přiděleny počítačům v dané subsíti.



Poznámka: Barva ikony odpovídá stavu adresy (viz dále). Ikona s písmenem R označuje IP adresy, které jsou rezervovány.

Sloupce okna *Přidělené IP adresy* obsahují následující informace:

- *IP adresa* — přidělená IP adresa
- *Skončení platnosti* — datum a čas skončení doby pronájmu této IP adresy
- *MAC adresa* — hardwarová adresa počítače, jemuž je IP adresa přidělena se jménem výrobce síťové karty.
- *Jméno počítače* — název počítače, kterému je IP adresa přidělena (pokud jej DHCP klient na tomto počítači DHCP serveru posílá)
- *Stav* — stav přidělení IP adresy: *Přiděleno* (adresa je přidělena klientovi a doba pronájmu dosud neskončila), *Expirováno* (doba pronájmu již uplynula a klient nepožádal o obnovení), *Odmítnuto* (klient odmítl přidělení této adresy) nebo *Uvolněno* (klient uvolnil přidělenou adresu).

  Poznámky:

  1. Informace o expirovaných a uvolněných IP adresách DHCP server udržuje pro případ, kdy příslušný klient opět požádá o přidělení IP adresy — DHCP server

se snaží přidělovat jednomu klientovi stále tutéž adresu. V případě nedostatku volných IP adres však mohou být tyto adresy přiděleny jiným klientům.

2. S odmítnutými IP adresami DHCP server zachází dle nastavení v záložce *Upřesňující volby* — viz dále.

Následující sloupce jsou ve výchozím nastavení skryty:

- *Čas posledního požadavku* — datum a čas, kdy klient vyslal poslední požadavek na přidělení či obnovení adresy
- *Zbývající doba přidělení* — doba zbývající od aktuálního času do *Skončení platnosti*

Tlačítko *Uvolnit* slouží k okamžitému uvolnění vybrané IP adresy (bez ohledu na její stav). Uvolněná adresa se ihned vrací do fondu volných adres a může být nabízena dalším klientům.

Tlačítkem *Rezervovat* můžete rezervovat vybranou (dynamicky přidělenou) IP adresu pro počítač, jemuž je aktuálně přidělena. Po stisknutí tohoto tlačítka dojde k automatickému přepnutí do záložky *Rozsahy adres* a zobrazí se dialog pro rezervaci adresy, jehož položky jsou již vyplněny odpovídajícími údaji (s výjimkou položky *Popis*). Po doplnění popisu a stisknutí tlačítka *OK* je IP adresa trvale rezervována pro počítač, kterému byla původně dynamicky přidělena.

Poznámka: Do dialogu pro rezervaci IP adresy je automaticky dosazena MAC adresa počítače, kterému je daná IP adresa přidělena. Chcete-li IP adresu rezervovat pro jméno počítače, změňte nastavení položek *Rezervovat pro* a *Hodnota*.

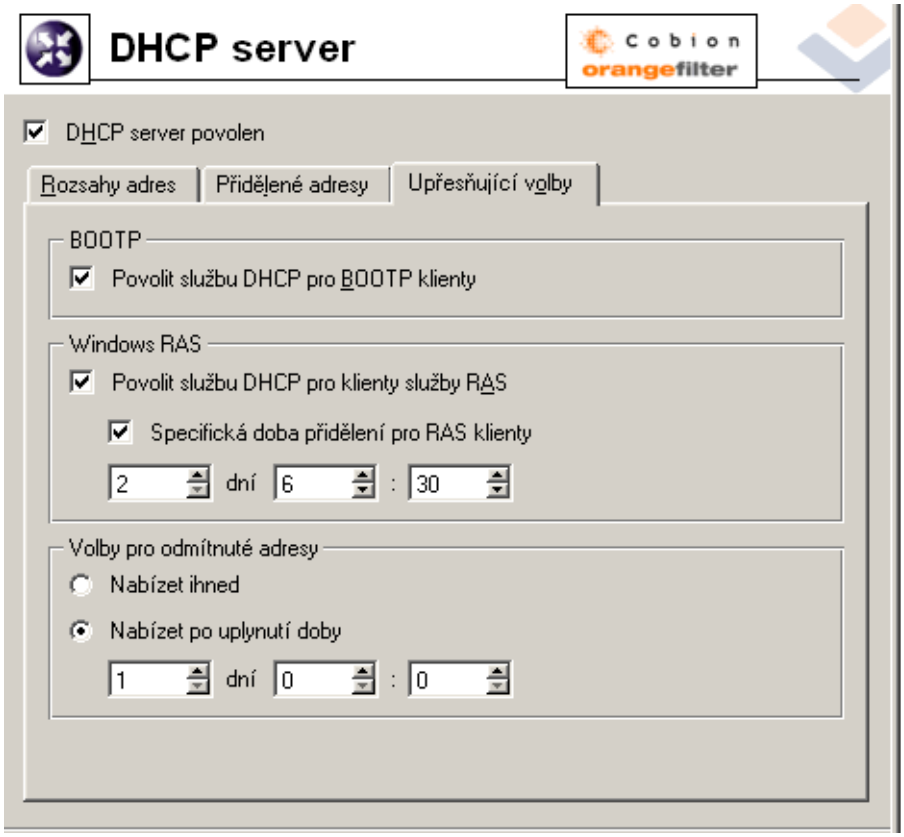
Upřesňující volby

Záložka *Upřesňující volby* slouží k nastavení některých dalších parametrů DHCP serveru.

BOOTP Zapnutím této volby bude DHCP server přidělovat IP adresy (včetně volitelných parametrů) také klientům protokolu BOOTP (předchůdce DHCP — přiděluje konfiguraci pouze staticky na základě MAC adresy).

Windows RAS Volba umožňuje povolit službu DHCP pro klienty RAS (Remote Access Service). Dále lze nastavit dobu přidělení pro RAS klienty, pokud nevyhovuje výchozí nastavení této hodnoty.

Volby pro odmítnuté adresy Nastavení v této sekci určuje, jakým způsobem budou obsluhovány IP adresy, které byly klienty odmítnuty (zpráva *DHCPDECLINE*). Tyto IP adresy mohou být buď okamžitě považovány za volné a v případě potřeby přiděleny



dalším klientům (volba *Nabízet ihned*) nebo po určitou dobu blokovány pro případ, že o ně původní klienti znovu požádají (volba *Nabízet po uplynutí doby*).

4.4 Proxy server

WinRoute obsahuje klasický HTTP proxy server, přestože umožňuje díky technologii NAT přímý přístup do Internetu ze všech počítačů v lokální síti. Avšak v některých případech není použití přímého přístupu vhodné nebo jej nelze použít vůbec. Jedná se zejména o tyto situace:

1. Z počítače s *WinRoute* není možné přímé připojení, je třeba použít proxy server poskytovatele Internetu.

   Proxy server ve *WinRoute* umí využívat tzv. nadřazený proxy server (*parent proxy server*), kterému předává veškeré požadavky.

2. Připojení do Internetu je realizováno vytáčenou linkou a přístup na určité WWW stránky je blokován (viz kapitola 6.1). Při použití přímého přístupu dojde k vytočení linky dříve, než může být zachycen vlastní HTTP požadavek (linka je vytáčena

na DNS dotaz nebo při požadavku klienta na navázání spojení s WWW serverem). Při přístupu na zakázanou WWW stránku *WinRoute* vytočí linku a poté zablokuje přístup na požadovanou stránku — linka je vytočena zbytečně.

Proxy server dokáže přijmout a zpracovat požadavek klienta lokálně. Jedná-li se o zakázanou stránku, k vytočení linky nedojde.

3. *WinRoute* je nasazen do sítě s velkým počtem počítačů, kde byl dříve používán proxy server. Změna konfigurace všech počítačů by byla časově i technicky náročná.

   Při použití proxy serveru zůstává přístup do Internetu funkční — konfigurace jednotlivých počítačů může zůstat nezměněna (případně lze změnit nastavení pouze na některých počítačích).

Upozornění: Proxy server ve *WinRoute* podporuje pouze protokol HTTP. Pro komunikaci protokolem FTP je třeba použít přímý přístup (tzn. nepoužívat proxy server)! Jedinou výjimkou je situace, kdy je použit nadřazený proxy server, který protokol FTP podporuje — proxy server ve *WinRoute* pak dokáže „tunelovat“ FTP na nadřazený proxy server.

Konfigurace proxy serveru

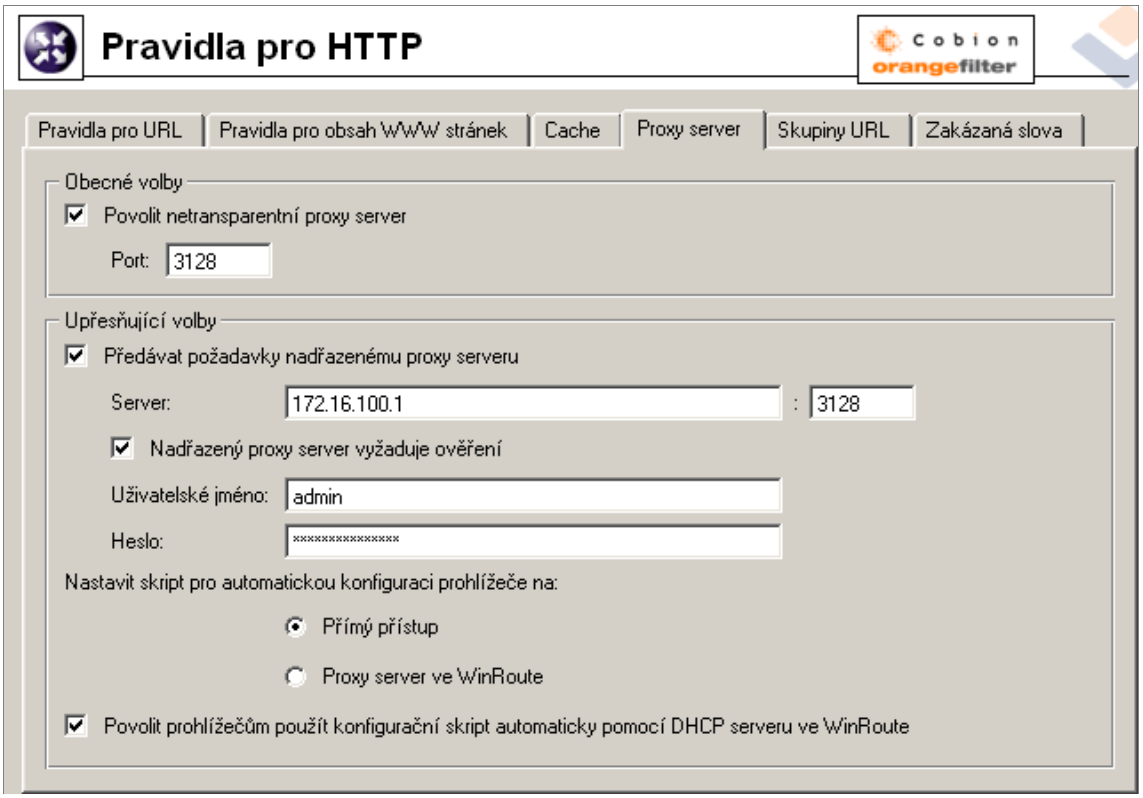
Parametry proxy serveru se nastavují v sekci *Konfigurace / Filtrování obsahu / Pravidla pro HTTP*, záložka *Proxy server*.

Povolit netransparentní proxy server Tato volba zapíná HTTP proxy server ve *WinRoute* na portu uvedeném v položce *Port* (výchozí port je `3128`).

Upozornění: Zadáme-li do položky *Port* číslo portu, který již používá jiná služba či aplikace, pak po stisknutí tlačítka *Použít WinRoute* tento port sice akceptuje, ale proxy server na něm nespustí a do záznamu *Error* (viz kapitola 12.4) se vypíše následující chybové hlášení:

```
failed to bind to port 3128: another application is using this
port
```

Pokud nemáte jistotu, že zadaný port je skutečně volný, pak bezprostředně po stisknutí tlačítka *Použít* zkontrolujte záznam *Error*, zda se v něm takovéto hlášení neobjevilo.



Předávat požadavky nadřazenému ... Zapnutím této volby bude proxy server ve *WinRoute* předávat veškeré požadavky nadřazenému proxy serveru specifikovanému v následujících položkách:

- *Server* — DNS jméno nebo IP adresa nadřazeného proxy serveru a port, na kterém běží (výchozí port je 3128)
- *Uživatelské jméno*, *Heslo* — uživatelské jméno a heslo pro ověření na nadřazeném proxy serveru.

  Volba zároveň slouží k automatickému nastavení přístupu antiviru *McAfee* a *Cobion Orange Filter* do Internetu přes tento proxy server.

  Nevyžaduje-li nadřazený proxy server ověření uživatele jménem a heslem, ponechte položky *Uživatelské jméno* a *Heslo* prázdné.

  Poznámka: Jméno a heslo pro ověření na nadřazeném proxy serveru se posílá s každým HTTP požadavkem. Je podporováno pouze ověřování typu *Basic*.

Povolit prohlížečům použít ... Pro použití proxy serveru je nutné správně nastavit parametry WWW prohlížečů na klientských počítačích. Většina prohlížečů umožňuje tyto parametry nastavovat automaticky. Po zapnutí volby *Povolit prohlížečům použít*

konfigurační skript automaticky pomocí DHCP serveru ve WinRoute lze využít tyto možnosti:

- Prohlížeč *Microsoft Internet Explorer* se konfiguruje zcela automaticky použitím DHCP serveru. V nastavení prohlížeče stačí zapnout volbu *Automaticky zjišťovat nastavení* (*Automatically detect settings*).

  Poznámka: Tento způsob automatické konfigurace vyžaduje, aby byl ve *WinRoute* spuštěn DHCP server (viz kapitola 4.3).

- Jiné prohlížeče (např. *Netscape/Mozilla*, *Opera* apod.) umožňují zadat URL skriptu pro automatickou konfiguraci. Toto URL má tvar:

  ```
  http://192.168.1.1:3128/pac/proxy.pac
  ```

  kde `192.168.1.1` je IP adresa počítače s *WinRoute* a `3128` je port proxy serveru (viz výše).

Volba *Nastavit skript pro automatickou konfiguraci prohlížeče na* určuje, jak mají být prohlížeče automaticky konfigurovány:

- *Přímý přístup* — prohlížeč bude nastaven tak, aby nepoužíval proxy server
- *Proxy server ve WinRoute* — v prohlížeči bude nastaven proxy server na IP adrese počítače s *WinRoute* a portu zvoleném v položce *Port* (viz výše).

Takto lze jediným kliknutím nastavit všechny prohlížeče na počítačích v lokální síti.

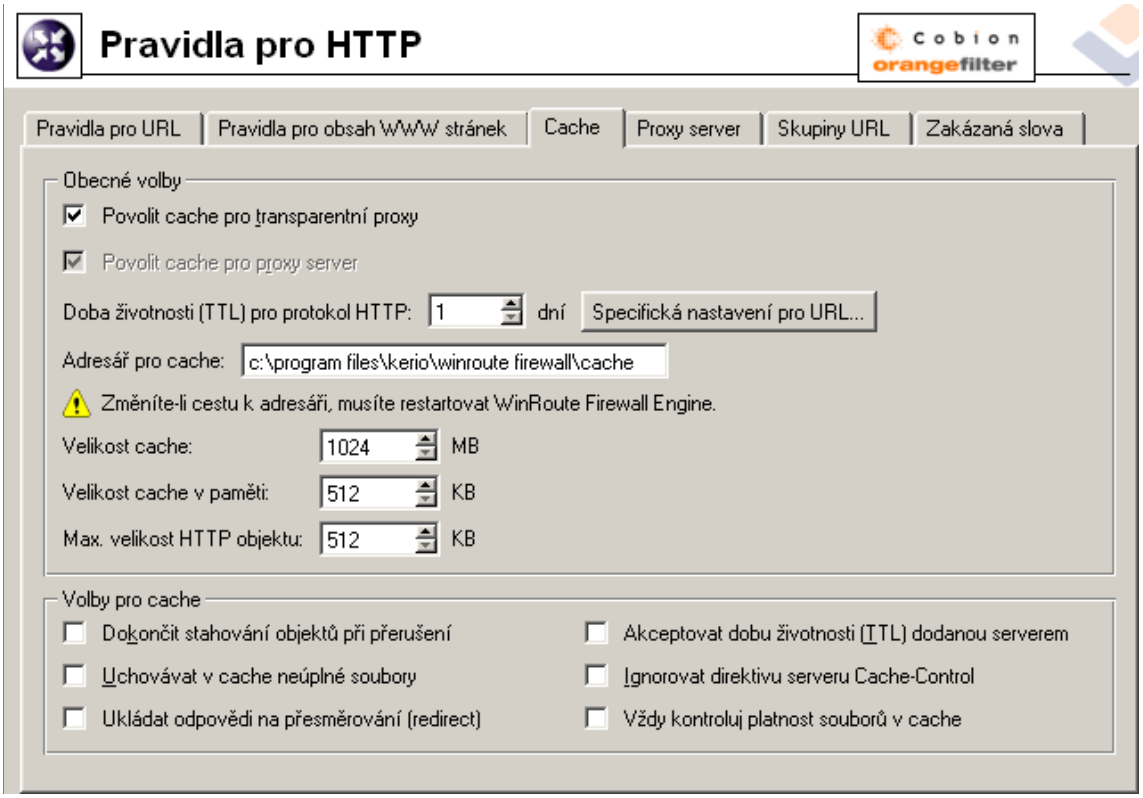
4.5 HTTP cache

Cache slouží ke zrychlení přístupu na opakovaně navštěvované WWW stránky a snížení zatížení internetového připojení (v případě měřené linky se také sníží objem přenesených dat). Stahované soubory se ukládají na disk počítače s *WinRoute* a při dalším přístupu nemusejí být znovu stahovány z WWW serveru.

Objekty se do cache ukládají na omezenou dobu (*Time To Live — TTL*). Tato doba určuje, zda se má na WWW serveru ověřovat novější verze daného objektu. Pokud doba *TTL* nevypršela, objekt se vezme z cache. V opačném případě se ověří, zda se objekt na příslušném WWW serveru změnil, a pokud ano, stáhne se nová verze. Tento mechanismus zajišťuje průběžnou aktualizaci objektů v cache.

Cache lze použít při přístupu přes proxy server i přímém přístupu. V případě přímého přístupu musí být na komunikaci aplikován inspekční modul HTTP (viz kapitoly 5.2 a 8.3).

Parametry HTTP cache se nastavují v sekci *Konfigurace / Filtrování obsahu / Pravidla pro HTTP*, záložka *Cache*.



Povolit cache pro transparentní proxy Zapnutí cache pro HTTP komunikaci obsluhovanou inspekčním modulem HTTP (tj. přímý přístup do Internetu)

Povolit cache pro proxy server Zapnutí cache pro objekty stahované přes proxy server ve *WinRoute* (viz kapitola 4.4)

Doba životnosti (TTL)... Výchozí doba platnosti objektu v cache. Tato doba je použita, jestliže:

- pro konkrétní objekt není nastavena specifická doba životnosti (nastavuje se v dialogu, který se otevírá tlačítkem *Specifická nastavení pro URL* — viz dále)
- není akceptována doba životnosti určená WWW serverem (viz položka *Akceptovat dobu životnosti (TTL) dodanou serverem*)

Adresář pro cache Adresář pro ukládání objektů. Ve výchozím nastavení se používá podadresář `cache` v adresáři, kde je *WinRoute* nainstalován.

Upozornění: Změna adresáře pro cache se projeví až po přístím startu *WinRoute Firewall Engine*.

Velikost cache Velikost souboru cache na disku. Maximální velikost tohoto souboru je dána použitým souborovým systémem: *FAT16* — 2GB, ostatní souborové systémy — 4GB.

Poznámka: Je-li cache zaplněna z 98%, spustí se automaticky tzv. úklid — smazání všech objektů, jejichž doba životnosti již vypršela. Nepodaří-li se odstranit žádné objekty, nebudou do cache ukládány nové objekty, dokud se místo neuvolní (při některém z dalších úklidů nebo ručním vymazáním).

Velikost cache v paměti Maximální velikost cache v operační paměti. Tato cache slouží zejména pro urychlení zápisu do cache na disku.

Příliš vysoká hodnota může mít negativní vliv na výkon počítače (velikost cache by neměla přesáhnout cca 10% velikosti operační paměti).

Max. velikost HTTP objektu Maximální velikost objektu, který bude do cache uložen.

Statistiky dokazují, že největší počet požadavků je na objekty malé velikosti (např. HTML stránky, obrázky apod.). Velké objekty, např. archivy, které se zpravidla stahují jednorázově, by v cache zbytečně zabíraly místo.

Volby pro cache Upřesňující nastavení chování cache.

- *Dokončit stahování objektů při přerušení* — po zaškrtnutí této volby se bude automaticky dokončovat stahování objektů, jestliže byl požadavek uživatelem přerušen (tlačítkem *Stop* ve WWW prohlížeči). Ve velkém počtu případů totiž uživatel přerušuje otevírání stránky z důvodu příliš pomalého natahování. Rozhodne-li se uživatel navštívit stránku znovu (případně ji navštíví jiný uživatel), bude stránka k dispozici nesrovnatelně rychleji.

- *Uchovávat v cache neúplné soubory* — zapnutím této volby bude server do cache ukládat i nekompletní objekty (jejichž stahování bylo přerušeno). Natahování stránky při opakované návštěvě pak bude o něco rychlejší.

  Je-li zapnuta volba *Dokončit stahování objektů při přerušení*, pak bude volba *Uchovávat v cache neúplné soubory* ignorována.

- *Ukládat odpovědi na přesměrování (redirect)* — po zapnutí této volby budou do cache ukládány HTTP odpovědi obsahující přesměrování.

- *Akceptovat dobu životnosti (TTL) dodanou serverem* — tato volba způsobí uložení objektů do cache na dobu doporučenou WWW serverem, ze kterého jsou objekty stahovány. Pokud server tuto dobu neurčí, použije se výchozí doba (viz položka *Doba životnosti (TTL) pro protokol HTTP*).

Upozornění: Některé WWW servery mohou záměrně dodávat příliš krátké nebo příliš dlouhé doby za účelem potlačení cache.

- *Ignorovat direktivu serveru Cache-Control* — po zapnutí této volby bude *WinRoute* ignorovat direktivy pro řízení cache na WWW stránkách.

  Pokud se obsah nějaké stránky velmi často mění, její autor na ni zpravidla umístí direktivu, aby se neukládala do cache. V některých případech je tato direktiva používána nerozumně, např. za účelem vyřazení cache. Volba *Ignorovat direktivu serveru Cache-Control* způsobí, že *WinRoute* bude akceptovat pouze direktivy *no-store* a *private*.

  Poznámka: WinRoute pracuje pouze s direktivami z hlaviček HTTP odpovědí, nikoliv ze samotných stránek.

- *Vždy kontroluj platnost souborů v cache* — zapnutím této volby bude *WinRoute* při každém požadavku kontrolovat, zda se na serveru nenachází novější verze objektu uloženého v cache (bez ohledu na to, zda to klient požaduje).

Poznámka: Klient si může kdykoliv vyžádat kontrolu novější verze objektu na WWW serveru (bez ohledu na nastavení cache). V prohlížečích *Microsoft Internet Explorer* a *Netscape/Mozilla* se to provede stisknutím kombinace kláves *Ctrl-F5*. Prohlížeče lze také nastavit, aby kontrolovaly novější verze stránek při každém přístupu (pak stačí stránku pouze obnovit).

Specifická nastavení pro URL

Výchozí doba životnosti objektu v cache nemusí být vyhovující pro všechny stránky. V některých případech může vzniknout požadavek neukládat stránku (resp. objekt) do cache vůbec či zkrátit dobu jeho platnosti (např. pro stránky, které se mění několikrát denně).

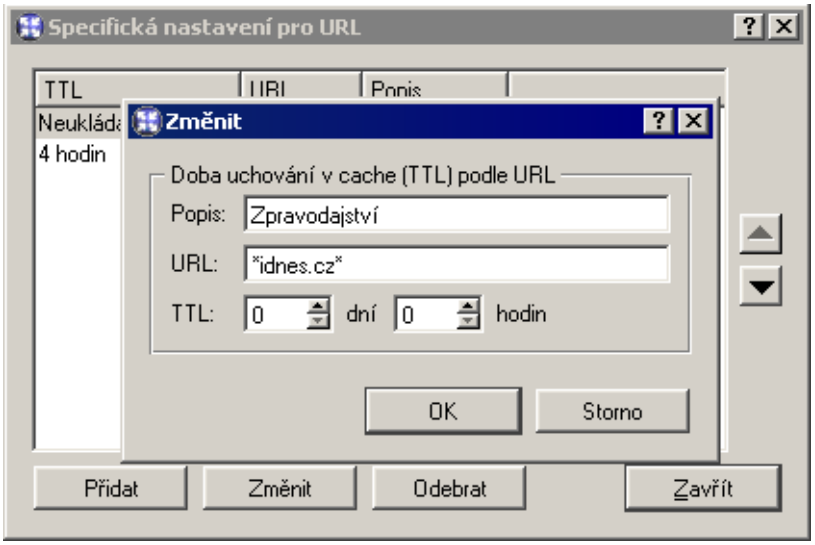
Tlačítko *Specifická nastavení pro URL* otevírá dialog, ve kterém lze nastavit dobu platnosti pro konkrétní URL.

Pravidla v tomto dialogu tvoří uspořádaný seznam, který je procházen shora dolů (tlačítky se šipkami na pravé straně okna lze upravit pořadí pravidel).

Popis Textový popis položky (pro snazší orientaci)

URL URL, pro které má být nastavena specifická doba životnosti objektů v cache. URL může být zadáno v jednom z těchto tvarů

- kompletní URL (např. `www.kerio.com/cz/index.html`)



- podřetězec s použitím hvězdičkové konvence (např. `*idnes.cz*`)
- jméno serveru (např. `www.kerio.com`) — libovolné URL na tomto serveru (zadaný řetězec se automaticky doplní na tvar: `www.kerio.com/*`)

TTL Doba platnosti objektů vyhovujících uvedenému URL.

Volba *0 dní, 0 hodin* znamená, že objekty nebudou do cache ukládány.

Kapitola 5

Komunikační pravidla

Komunikační pravidla (*Traffic Policy*) jsou základem konfigurace *WinRoute*. V jediné tabulce je integrováno nastavení:

- zabezpečení (tj. ochrany lokální sítě včetně počítače, na němž je *WinRoute* nainstalován, proti nežádoucímu průniku z Internetu)
- překladu IP adres (též NAT, Network Address Translation — technologie umožňující transparentní přístup z celé lokální sítě do Internetu prostřednictvím jediné veřejné IP adresy)
- zpřístupnění serverů (služeb) běžících v lokální síti z Internetu (tzv. mapování portů)
- řízení přístupu lokálních uživatelů do Internetu

K definici komunikačních pravidel slouží sekce *Konfigurace / Komunikační pravidla*. Pravidla mohou být definována dvěma způsoby: ručně (pro zkušené správce) nebo pomocí průvodce (pro méně zkušené uživatele nebo případy, kdy nejsou třeba žádná speciální nastavení).

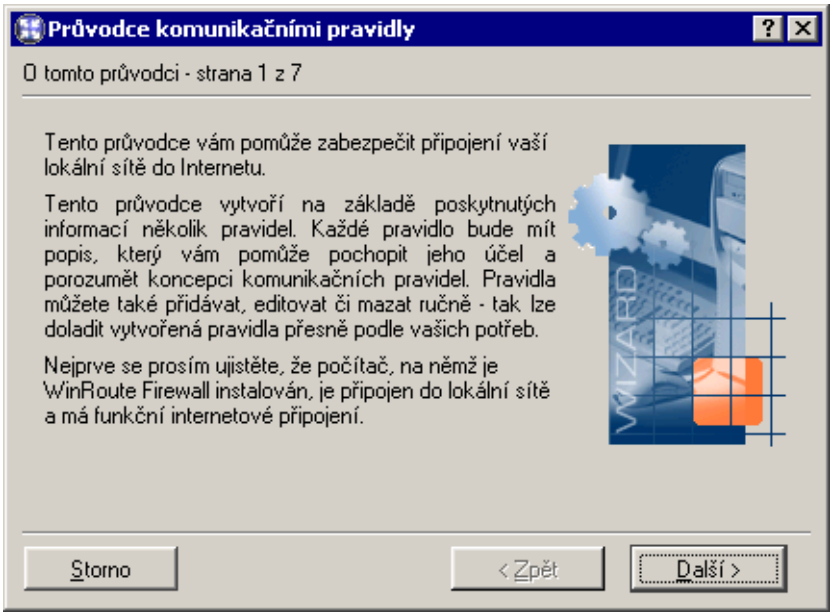
5.1 Průvodce komunikačními pravidly

Průvodce (wizard) se uživatele dotáže pouze na nejnutnější informace, na jejichž základě vytvoří sadu komunikačních pravidel. Vytvořená pravidla zajistí přístup z lokální sítě do Internetu ke zvoleným službám, přístup z Internetu k vybraným lokálním serverům a plnou ochranu lokální sítě (včetně počítače s *WinRoute*) proti neoprávněnému přístupu z Internetu. Aby bylo možné zaručit funkčnost *WinRoute* po použití průvodce, jsou před dokončením průvodce všechna stávající pravidla smazána a nahrazena pravidly vytvořenými automaticky na základě poskytnutých informací.

Průvodce komunikačními pravidly se spustí stisknutím tlačítka *Průvodce*.

Poznámka: Nahrazení stávajících komunikačních pravidel pravidly vytvořenými průvodcem se provádí až po potvrzení posledního kroku. Průvodce tedy můžete v kterémkoliv kroku stornovat beze ztráty stávajících pravidel.

Krok 1 — informace

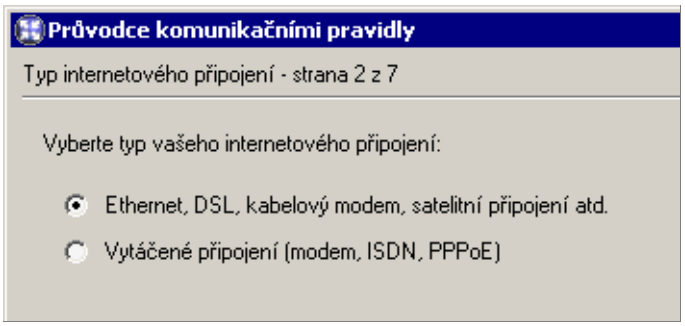


Průvodce předpokládá, že počítač, kde je *WinRoute* nainstalován, je vybaven:

- alespoň jedním aktivním adaptérem pro lokální síť
- alespoň jedním aktivním adaptérem připojeným do Internetu nebo je definováno alespoň jedno vytáčené připojení. Vytáčená linka nemusí být v okamžiku spuštění průvodce připojena.

Krok 2 — výběr typu internetového rozhraní

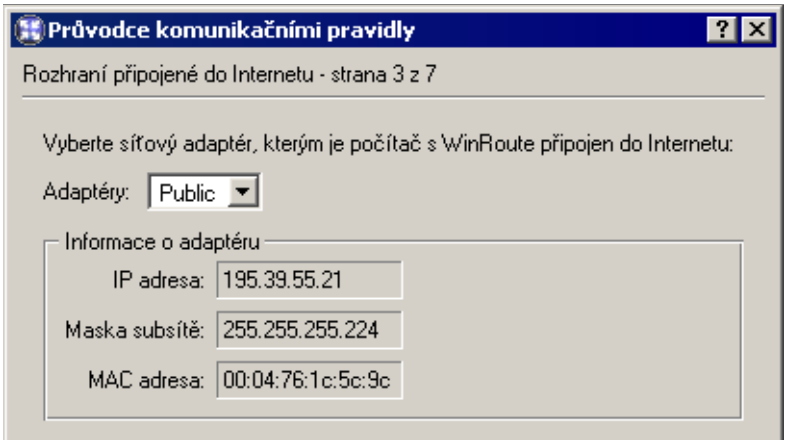
Vyberte způsob, jakým je počítač s *WinRoute* připojen do Internetu: síťovým adaptérem (Ethernet, WaveLAN, DSL apod.) nebo vytáčenou linkou (analogový modem, ISDN atd.).



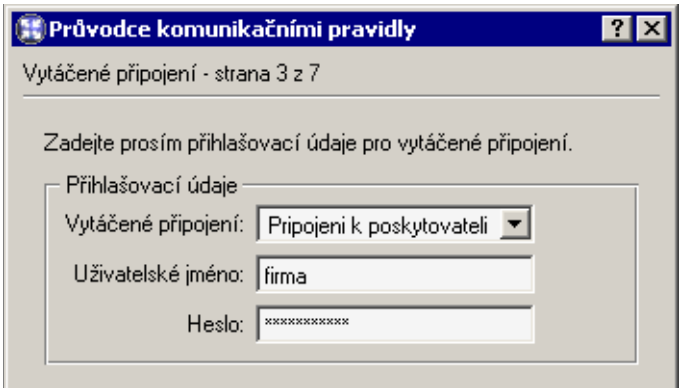
Krok 3 - výběr internetového adaptéru nebo vytáčené linky

Je-li počítač připojen do Internetu síťovým adaptérem, stačí jej vybrat ze seznamu. V průvodci se pro snazší orientaci zobrazuje také IP adresa, maska subsítě a MAC adresa zvoleného adaptéru.

Poznámka: Na prvním místě seznamu je nabízeno internetové rozhraní s výchozí bránou. Proto je ve většině případů v tomto kroku již přednastaven správný adaptér.



Pro vytáčenou linku, je třeba vybrat příslušné telefonické připojení (definované v operačním systému) a zadat odpovídající uživatelské jméno a heslo.



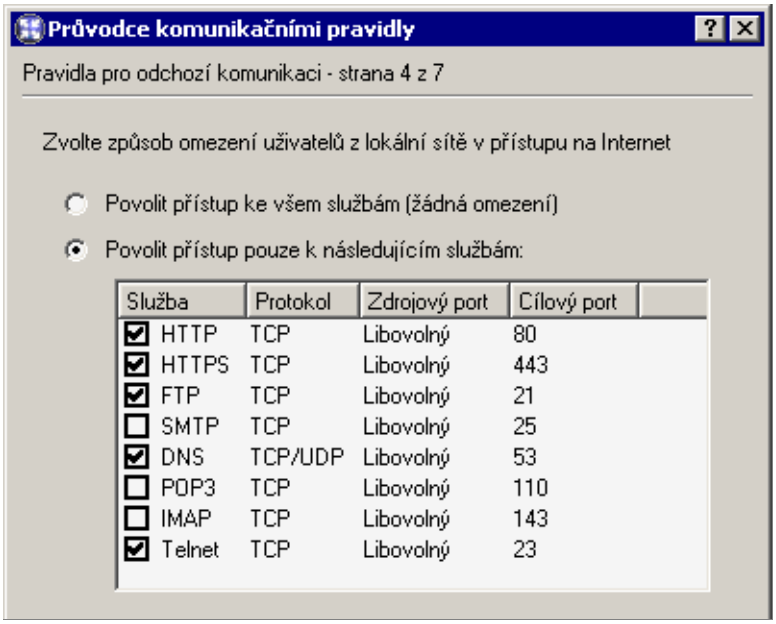
Krok 4 — omezení přístupu na Internet

Zvolte, k jakým službám v Internetu budou uživatelé z lokální sítě smět přistupovat:

Povolit přístup ke všem službám Přístup z lokální sítě do Internetu nebude nijak omezen. Uživatelé budou smět využívat jakoukoliv službu běžící na serveru v Internetu.

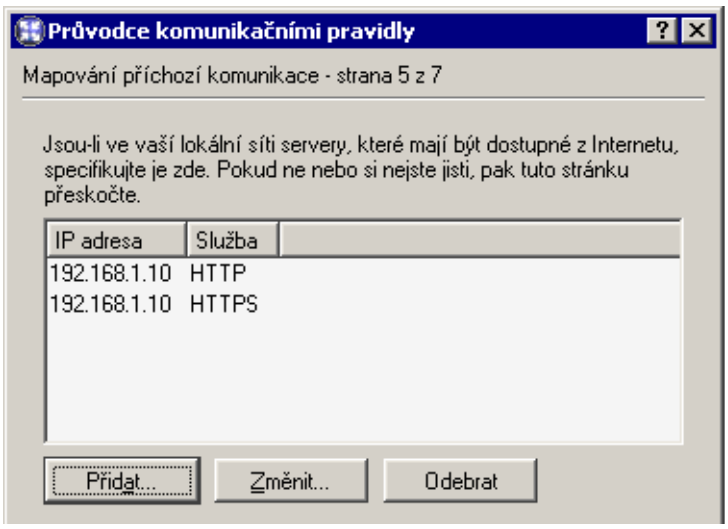
Povolit přístup pouze k následujícím službám Z lokální sítě bude povolen přístup pouze ke službám, které zde vyberete.

Poznámka: V tomto dialogu je uveden výčet pouze základních služeb (nezávisle na tom, jaké služby jsou ve *WinRoute* definovány — viz kapitola 8.3). Další služby můžete povolit přidáním vlastních komunikačních pravidel — viz kapitola 5.2.

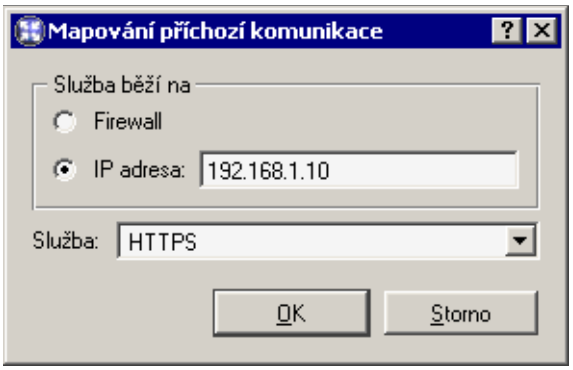


Krok 5 — zpřístupnění služeb v lokální síti

Běží-li na počítači s *WinRoute* či na některém počítači v lokální síti služba (např. WWW server, FTP server apod.), kterou chcete zpřístupnit z Internetu, definujte ji v tomto dialogu.



Tlačítko *Přidat* otevírá dialog pro zpřístupnění nové služby.



Služba běží na Volba počítače, na němž služba běží:

- *Firewall* — počítač, na němž je *WinRoute* nainstalován
- *IP adresa* — adresa serveru v lokákní síti (počítač, na kterém služba běží)

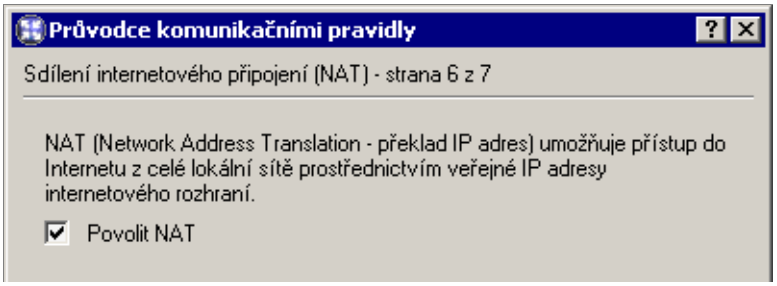
  Poznámka: Výchozí brána na tomto počítači musí být nastavena tak, aby přistupoval do Internetu přes *WinRoute* — jinak nebude zpřístupnění služby fungovat!

Služba Výběr služby, která má být zpřístupněna. Tato služba musí být nejprve definována v sekci *Konfigurace / Definice / Služby* (viz kapitola 8.3).

Poznámka: Většina běžných služeb je ve *WinRoute* již předdefinována.

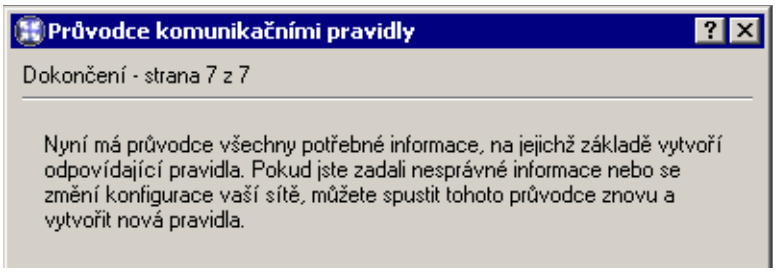
Krok 6 — NAT

Pokud se jedná o privátní lokální síť, která má být připojena do Internetu přes jedinou veřejnou IP adresu, zapněte funkci *NAT* (překlad IP adres). Je-li *WinRoute* použit pro směrování mezi dvěma veřejnými sítěmi či mezi dvěma lokálními segmenty (tzv. neutrální směrovač), pak překlad adres nezapínejte.



Krok 7 — vytvoření pravidel

V posledním kroku vás průvodce informuje o tom, že vytvoří komunikační pravidla na základě shromážděných informací. Všechna stávající pravidla budou smazána a nahrazena nově vytvořenými pravidly.



Upozornění: Toto je poslední možnost průvodce stornovat a zachovat stávající komunikační pravidla! Po stisknutí tlačítka *Dokončit* budou smazána a nahrazena novými.

Pravidla vytvořená průvodcem

Podívejme se podrobněji na komunikační pravidla, která byla vytvořena průvodcem v předchozím příkladu.

Komunikační pravidla

Jméno	Zdroj	Cíl	Služba	Akce	Zazn	Překlad
ICMP komunikace	Firewall	Libovolný	Ping	✓		
NAT	LAN	Internet	HTTP HTTPS FTP DNS Telnet	✓		NAT (Výchozí výstupní rozhraní)
Lokální komunikace	Firewall LAN	Firewall LAN	Libovolný	✓		
Komunikace firewallu	Firewall	Internet	HTTP HTTPS FTP DNS Telnet	✓		
Služba HTTP	Internet	Firewall	HTTP	✓		Mapování 192.168.1.10
Služba HTTPS	Internet	Firewall	HTTPS	✓		Mapování 192.168.1.10
Implicitní pravidlo	Libovolný	Libovolný	Libovolný	✗		

ICMP komunikace Toto pravidlo je průvodcem přidáno vždy, bez ohledu na nastavení v jednotlivých krocích. Umožňuje *PING* (tj. vyslání žádosti o odezvu) z počítače,

kde je *WinRoute* nainstalován. *PING* je velmi důležitý např. pro ověření funkčnosti internetového připojení.

Poznámka: Pravidlo *ICMP komunikace* nepovoluje *PING* z počítačů v lokální síti do Internetu. Je-li to požadováno, je třeba přidat službu *Ping* do pravidla *NAT* (detaily viz kapitola 5.2).

NAT Toto pravidlo určuje, že ve všech paketech jdoucích z lokální sítě do Internetu bude zdrojová (privátní) IP adresa nahrazována adresou rozhraní připojeného do Internetu (v průvodci krok 3 a krok 6). Přístup bude povolen pouze k vybraným službám (krok 4).

Lokální komunikace Toto pravidlo povoluje veškerou komunikaci počítačů v lokální síti s počítačem, na němž *WinRoute* běží. Položky *Zdroj* a *Cíl* v tomto pravidle zahrnují všechna rozhraní počítače s *WinRoute* kromě rozhraní připojeného do Internetu (vybraného v kroku 3).

Poznámka: Průvodce předpokládá, že počítač s *WinRoute* logicky patří do lokální sítě, a přístup k němu nijak neomezuje. Omezení přístupu na tento počítač lze provést úpravou pravidla nebo definicí nového. Je nutné si uvědomit, že nevhodné omezení přístupu k počítači s *WinRoute* může mít za následek zablokování vzdálené správy či nedostupnost služeb v Internetu (veškerá komunikace do Internetu prochází přes tento počítač).

Komunikace firewallu Toto pravidlo povoluje přístup k vybraným službám z počítače, kde je *WinRoute* nainstalován. Je obdobou pravidla *NAT*, ale s tím rozdílem, že se zde neprovádí překlad IP adres (tento počítač má přímý přístup do Internetu).

Služba HTTP a Služba HTTPS Tato dvě pravidla zpřístupňují (mapují) služby *HTTP* a *HTTPS* běžící na počítači s IP adresou `192.168.1.10` (krok 6). Tyto služby budou z Internetu přístupné na IP adresách vnějšího rozhraní (krok 3).

Implicitní pravidlo Toto pravidlo zakazuje veškerou komunikaci, která není povolena jinými pravidly. Implicitní pravidlo je vždy na konci seznamu komunikačních pravidel a nelze jej odstranit.

Implicitní pravidlo umožňuje zvolit akci pro nežádoucí komunikaci (*Zakázat* nebo *Zahodit*) a zapnout záznam paketů nebo spojení.

Poznámka: Detailní popis jednotlivých částí komunikačního pravidla najdete v kapitole 5.2.

5.2 Definice vlastních komunikačních pravidel

Chcete-li dále doladit nastavení *WinRoute*, můžete definovat vlastní pravidla, případně upravit pravidla vytvořená průvodcem. Zkušení správci nemusejí průvodce použít vůbec — mohou vytvořit kompletní sadu pravidel přesně podle specifických požadavků.

Poznámka: Chcete-li řídit přístup uživatelů k WWW a FTP serverům, doporučujeme namísto komunikačních pravidel použít speciální nástroje, které *WinRoute* k tomuto účelu nabízí — viz kapitola 6.

Jak komunikační pravidla fungují?

Komunikační pravidla jsou uložena v uspořádaném seznamu. Při aplikaci pravidel je seznam procházen shora dolů a použije se vždy první pravidlo, kterému dané spojení či paket vyhovuje — záleží tedy na pořadí pravidel v seznamu. Pořadí pravidel lze upravit šipkovými tlačítky v pravé části okna.

Na konci seznamu je vždy umístěno implicitní pravidlo, které zakazuje nebo zahazuje veškerou komunikaci (akce je volitelná). Toto pravidlo nelze odstranit. Komunikace, která není pravidly výslovně povolena, je zakázána.

Poznámka: Bez definice komunikačních pravidel (pomocí průvodce či vlastních) existuje ve *WinRoute* pouze implicitní pravidlo, které blokuje veškerou komunikaci.

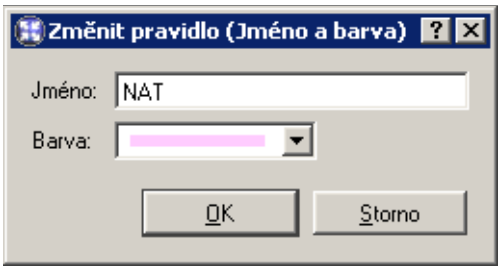
Definice pravidel

Komunikační pravidla jsou zobrazována ve formě tabulky, kde každý řádek obsahuje jedno pravidlo a ve sloupcích jsou jeho jednotlivé části (jméno, podmínky, akce — detaily viz dále). Dvojitým kliknutím levým tlačítkem myši na vybrané pole tabulky (případně kliknutím pravým tlačítkem a volbou *Změnit...* z kontextového menu) se zobrazí dialog pro změnu vybrané položky.

Nové pravidlo přidáme stisknutím tlačítka *Přidat* a šipkovými tlačítky v pravé části okna jej přesuneme na požadované místo.

Jméno Název pravidla. Měl by být stručný a výstižný, aby tabulka pravidel byla přehledná. Detailnější informace by měly být zapsány do položky *Popis*.

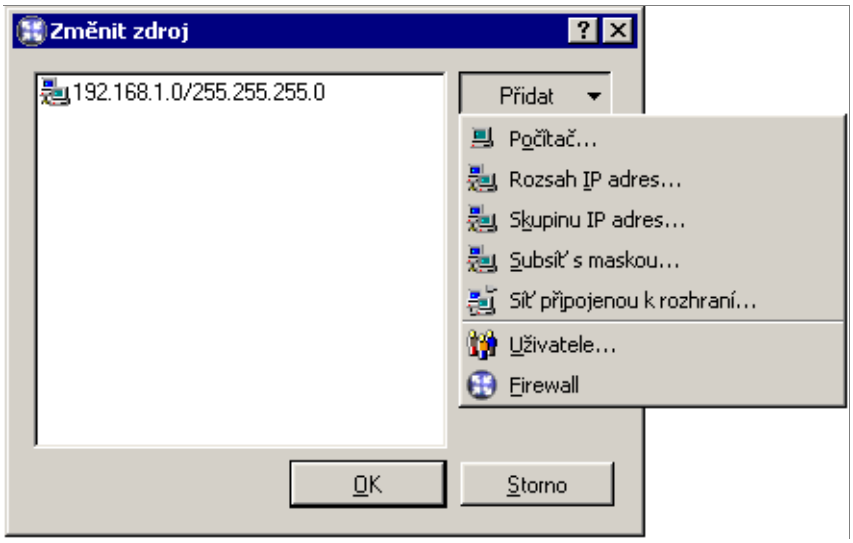
Zaškrtávací pole před jménem pravidla slouží k jeho aktivaci a deaktivaci. Není-li toto pole zaškrtnuto, pak se *WinRoute* chová, jako by pravidlo neexistovalo. Toho lze využít např. pro dočasné vyřazení pravidla — není třeba je odstraňovat a později znovu definovat.



Kromě výše uvedeného jména můžete nastavit také barvu pozadí řádku tabulky s tímto pravidlem. Volba *Transparentní* znamená, že řádek bude „průhledný“ (pod textem bude barva pozadí celého seznamu, typicky bílá).

Poznámka: Barva pravidla slouží pouze pro zlepšení přehlednosti — nesouvisí s jeho významem.

Zdroj, Cíl Volba zdroje, resp. cíle komunikace, pro niž má pravidlo platit.

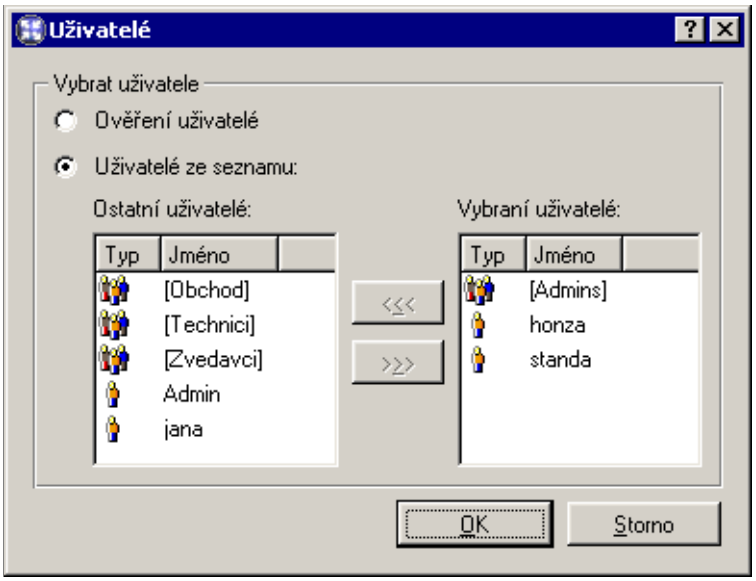


Tlačítkem *Přidat* lze definovat novou položku zdroje, resp. cíle komunikace:

- *Počítač* — IP adresa konkrétního počítače (např. `192.168.1.1`)
- *Rozsah IP adres* — např. `192.168.1.10`—`192.168.1.20`
- *Skupinu IP adres* — skupina adres definovaná ve *WinRoute* (viz kapitola 8.1)
- *Subsíť s maskou* — subsíť zadaná adresou sítě a maskou (např. `192.168.1.0/255.255.255.0`)

- *Síť připojenou k rozhraní* — výběr rozhraní, kterým paket přichází (v položce *Zdroj*) nebo kudy má být odeslán (v položce *Cíl*)

- *Uživatele* — uživatelé nebo skupiny uživatelů, které lze vybrat ve speciálním dialogu.



Volba *Ověření uživatelé* znamená, že podmínka bude platit pro všechny uživatele, kteří jsou na firewall již přihlášeni (viz kapitola 7.2).

V komunikačních pravidlech má uživatel (resp. skupina) význam IP adresy počítače, z něhož je přihlášen (podrobnosti o ověřování uživatelů na firewallu naleznete v kapitole 7.2).

Poznámky:

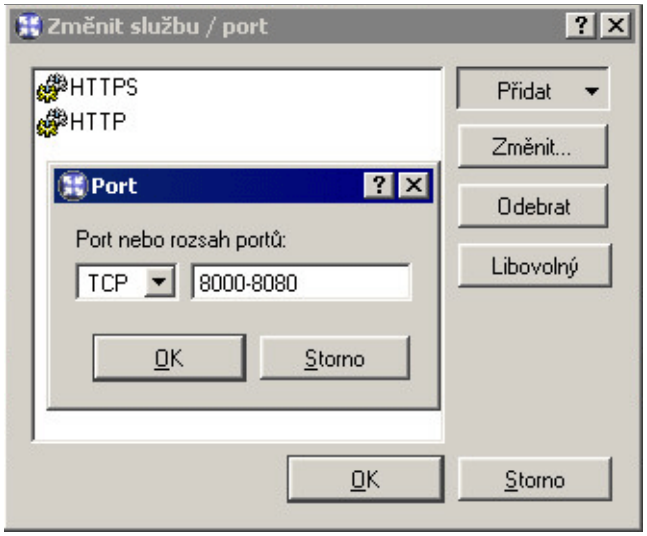
1. Povolení / zákaz přístupu určitým uživatelům má smysl jen tehdy, pokud je zavedeno globální omezení pro nepřihlášené uživatele (jinak totiž není uživatel donucen se přihlásit).

2. V případě služby HTTP umožňuje *WinRoute* vyžádat ověření uživatele automatickým přesměrováním na přihlašovací stránku (podrobnosti viz kapitola 6.1). U ostatních služeb toto možné není — je-li přístup ke službě omezen dle uživatelů a z daného počítače není přihlášen žádný uživatel, pak je služba blokována. Uživatelé by měli být informováni o tom, že před přístupem k takové službě musejí otevřít přihlašovací stránku (viz kapitoly 7 a 7.2) ve svém WWW prohlížeči a přihlásit se.

- *Firewall* — speciální skupina adres zahrnující všechna rozhraní počítače, na němž *WinRoute* běží. Tuto volbu lze s výhodou využít např. pro povolení komunikace mezi lokální sítí a počítačem s *WinRoute*.

Poznámka: Tlačítko *Libovolný* nahradí všechny definované položky položkou *Libovolný* (toto je rovněž výchozí hodnota při vytváření nového pravidla). Bude-li pak přidána alespoň jedna nová položka, bude položka *Libovolný* automaticky odstraněna.

Služba Definice služby (resp. služeb), pro kterou má toto komunikační pravidlo platit. Seznam může obsahovat více služeb definovaných v sekci *Konfigurace / Definice / Služby* a/nebo služeb zadaných protokolem a číslem portu (případně rozsahem portů — pro jeho specifikaci se zde používá pomlčka).



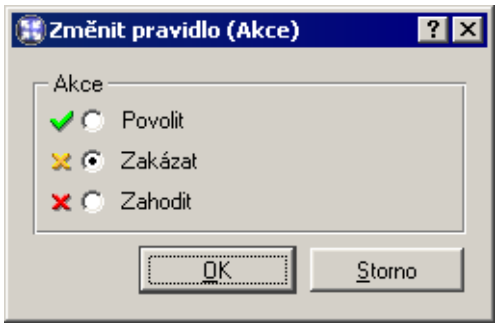
Poznámky:

1. Je-li v definici služby použit inspekční modul daného protokolu, pak se na komunikaci vyhovující tomuto pravidlu inspekční modul aplikuje. Pokud pravidlo platí pro všechny služby (tlačítko *Libovolný*), pak jsou automaticky aplikovány všechny potřebné inspekční moduly.

   Chceme-li docílit toho, aby na určitou komunikaci nebyl aplikován příslušný inspekční modul, je třeba definovat vlastní službu bez použití inspekčního modulu (detaily viz kapitola 8.3).

2. Tlačítko *Libovolný* nahradí všechny definované položky položkou *Libovolný* (toto je rovněž výchozí hodnota při vytváření nového pravidla). Bude-li pak přidána alespoň jedna nová služba, bude položka *Libovolný* automaticky odstraněna.

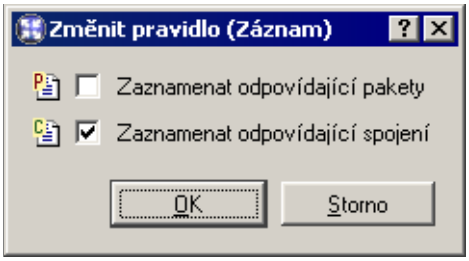
Akce Způsob, jak *WinRoute* obslouží komunikaci, která vyhoví podmínkám tohoto pravidla (podmínka je dána položkami *Zdroj*, *Cíl* a *Služba*). Možnosti jsou:



- *Povolit* — firewall komunikaci propustí
- *Zakázat* — firewall pošle klientovi (iniciátorovi komunikace) řídicí zprávu, že přístup na danou adresu či port je zakázán. Výhodou tohoto způsobu je okamžitá reakce, klient se však dozví o tom, že je komunikace blokována firewallem.
- *Zahodit* — firewall bude zahazovat veškeré pakety vyhovující danému pravidlu. Klientovi nebude poslána žádná řídicí zpráva a tuto situaci vyhodnotí jako síťovou chybu. Odezva klienta není v tomto případě okamžitá (určitou dobu čeká na odpověď, poté se případně snaží navázat spojení znovu atd.), existence firewallu mu však zůstane skryta.

Poznámka: Na základě výše popsaných skutečností doporučujeme při omezování lokálních uživatelů v přístupu na Internet používat volbu *Zakázat*, při blokování přístupu z Internetu naopak volbu *Zahodit*.

Zaznamenat O komunikaci, která vyhověla tomuto pravidlu, lze provést záznam následujícím způsobem:



- *Zaznamenat odpovídající pakety* — veškeré pakety, které vyhoví tomuto pravidlu (propuštěné, odmítnuté či zahozené — v závislosti na typu akce v pravidle) budou zaznamenány do záznamu *Filter*.

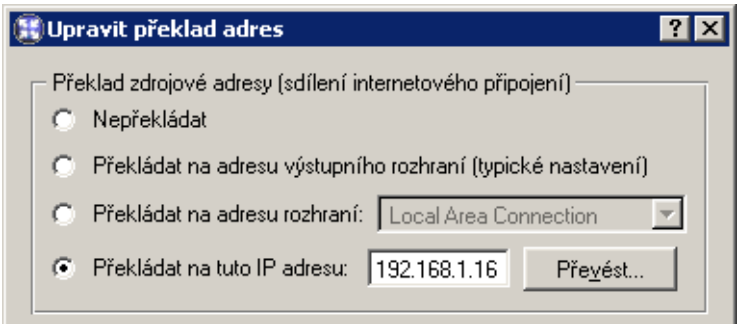
- *Zaznamenat odpovídající spojení* — všechna spojení vyhovující tomuto pravidlu budou zaznamenána do záznamu *Connection* (pouze v případě povolujícího pravidla). Jednotlivé pakety v rámci těchto spojení se již nezaznamenávají.

  Poznámka: U zakazujících a zahazujících pravidel nelze zaznamenávat spojení.

Překlad Způsob překladu zdrojové nebo cílové IP adresy (případně obou).

Překlad zdrojové adresy (NAT — *Network Address Translation*) se též nazývá maskování IP adresy nebo sdílení internetového připojení. V paketech jdoucích z lokální sítě do Internetu se zdrojová (privátní) IP adresa nahrazuje adresou rozhraní připojeného do Internetu. Celá lokální síť má tak transparentní přístup do Internetu, ale navenek se jeví jako jeden počítač.

Překlad zdrojové adresy se definuje následujícím způsobem:



- *Nepřekládat* — zdrojová adresa zůstává nezměněna. Toto je výchozí volba a v komunikačních pravidlech se nezobrazuje (pro přehlednost).

- *Překládat na adresu výstupního rozhraní* — v tomto případě *WinRoute* automaticky detekuje výstupní rozhraní podle cílové IP adresy v paketu.

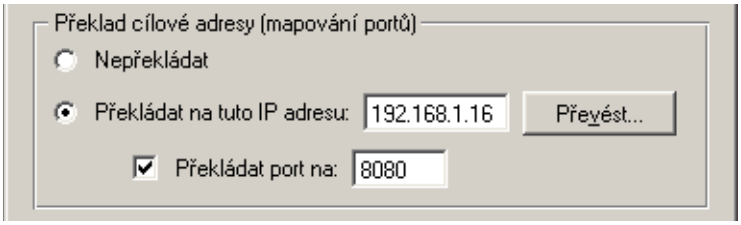
- *Překládat na adresu rozhraní* — výběr rozhraní, na jehož primární adresu bude zdrojová IP adresa paketu překládána. Tato volba je vhodná všude tam, kde se může výstupní rozhraní měnit (např. více vytáčených linek).

- *Překládat na tuto IP adresu* — zde lze zadat konkrétní IP adresu, na niž má být zdrojová adresa překládána (např. sekundární adresu rozhraní připojeného do Internetu). Pokud znáte pouze DNS jméno počítače, lze použít tlačítko *Převést*, které převede DNS jméno na IP adresu.

Upozornění: Je třeba uvést IP adresu, která je přiřazena některému rozhraní počítače s *WinRoute*!

Překlad cílové adresy (též mapování portů) slouží ke zpřístupnění služby běžící na počítači v privátní lokální síti zvenčí. Pokud příchozí paket vyhovuje daným podmínkám, je cílová adresa zaměněna a paket směrován na příslušný počítač. Tímto způsobem bude služba „přenesena“ na vnější rozhraní počítače s *WinRoute* (resp. na IP adresu, z níž je mapována). Z pohledu klienta v Internetu služba běží na IP adrese, ze které je mapována (tzn. obvykle na vnější adrese firewallu).

Nastavení překladu cílové adresy (mapování portů):



- *Nepřekládat* — cílová adresa zůstane nezměněna.
- *Překládat na tuto IP adresu* — IP adresa, na níž má být cílová adresa paketu změněna. Tato adresa je zároveň adresou počítače, kde daná služba skutečně běží. Pokud znáte pouze DNS jméno počítače, lze použít tlačítko *Převést*, které převede DNS jméno na IP adresu.
- *Překládat port na* — při záměně cílové adresy může být zaměněn i port dané služby. Služba tedy může fyzicky běžet na jiném portu, než ze kterého je mapována.

  Poznámka: Tuto volbu je možné použít jen v případě, je-li v položce *Služba* komunikačního pravidla uvedena pouze jedna služba a tato služba používá pouze jeden port nebo jeden rozsah portů.

Popis Tato položka může obsahovat libovolný text popisující význam a účel daného pravidla (maximálně 1024 znaků).

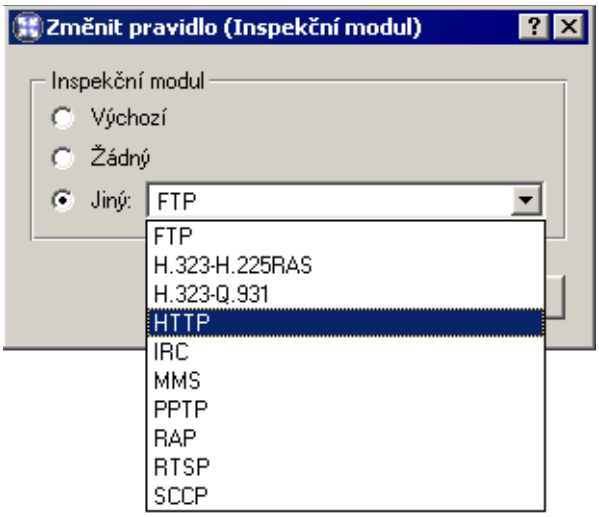
Doporučujeme důsledně popisovat všechna vytvořená pravidla (případně též komentovat pravidla vytvořená konfiguračním průvodcem). Ne vždy je totiž na první pohled zřejmé, k jakému účelu konkrétní pravidlo slouží. Dobré popisy pravidel ušetří správci *WinRoute* mnoho času při pozdějším ladění či hledání problémů.

Následující dva sloupce jsou ve výchozím nastavení okna *Komunikační pravidla* skryté:

Platí v Časový interval, ve kterém má pravidlo platit. Mimo tento časový interval se *WinRoute* chová tak, jako by pravidlo neexistovalo.

Speciální volba *vždy* vypíná časové omezení pravidla (v okně *Komunikační pravidla* se nezobrazuje).

Inspekční modul Volba inspekčního modulu, který má být aplikován na komunikaci vyhovující pravidlu. Možnosti jsou následující:



- *Výchozí* — na komunikaci vyhovující tomuto pravidlu budou aplikovány všechny potřebné inspekční moduly, případně inspekční moduly služeb uvedených v položce *Služba*.

- *Žádný* — nebude aplikován žádný inspekční modul (bez ohledu na to, jak jsou definovány služby použité v položce *Služba*).

- *Jiný* — výběr konkrétního inspekčního modulu, který má být pro komunikaci popsanou tímto pravidlem použit.

  Upozornění: Tuto volbu doporučujeme používat, pouze pokud komunikační pravidlo popisuje protokol, pro který je inspekční modul určen. Použití nesprávného inspekčního modulu může způsobit nefunkčnost dané služby.

Poznámka: Je-li v definici pravidla použita konkrétní služba (viz položka *Služba*), doporučujeme v položce *Inspekční modul* ponechat volbu *Výchozí* (inspekční modul je již zahrnut v definici služby).

5.3 Základní typy komunikačních pravidel

Komunikační pravidla ve *WinRoute* nabízejí poměrně široké možnosti filtrování síťového provozu a zpřístupnění služeb. V této kapitole uvedeme příklady komunikačních

pravidel řešících standardní situace. Podle těchto příkladů můžete snadno vytvořit sadu pravidel pro vaši konkrétní síťovou konfiguraci.

Překlad IP adres

Překlad IP adres (NAT) znamená záměnu zdrojové (privátní) IP adresy v paketu jdoucím z lokální sítě do Internetu za IP adresu vnějšího rozhraní počítače s *WinRoute*. Příslušné komunikační pravidlo může tedy vypadat následovně:

Zdroj Rozhraní, k němuž je připojena lokální privátní síť.

Jestliže je lokální síť tvořena více segmenty, z nichž každý je připojen k samostatnému rozhraní, uveďte do položky *Zdroj* všechna tato rozhraní.

Je-li lokální síť tvořena kaskádními segmenty (tzn. obsahuje další routery), stačí uvést pouze rozhraní, přes které je síť připojena k počítači s *WinRoute* (není třeba vyjmenovávat všechny subsítě, které lokální síť obsahuje).

Cíl Rozhraní připojené do Internetu.

Služba Tato položka může být použita ke globálnímu omezení přístupu do Internetu. Budou-li v pravidle pro překlad IP adres uvedeny konkrétní služby, pak bude překlad fungovat pouze pro tyto služby a ostatní služby v Internetu budou z lokální sítě nepřístupné.

Akce Musí být nastavena na *Povolit* (jinak by byla komunikace blokována a překlad adres by již neměl žádný smysl).

Překlad V sekci *Překlad zdrojové adresy* stačí vybrat volbu *Překládat na adresu výstupního rozhraní* (pro NAT se použije primární IP adresa rozhraní, přes které paket odchází z počítače s *WinRoute*).

Má-li být pro překlad použita jiná IP adresa, použijte volbu *Překládat na tuto IP adresu*, v níž uvedete požadovanou adresu. Zadaná IP adresa musí být jednou z adres přiřazených výstupnímu rozhraní, jinak nebude překlad IP adres fungovat správně.

Upozornění: V sekci *Překlad cílové adresy* by měla být nastavena volba *Nepřekládat*, jinak není zaručena zamýšlená funkce pravidla. Kombinace překladu zdrojové i cílové adresy má význam pouze ve speciálních případech.

Umístění pravidla Pravidlo pro překlad zdrojových adres musí být umístěno pod všemi pravidly, která omezují přístup z lokální sítě do Internetu.

Poznámka: Takto definované pravidlo povoluje přístup do Internetu z počítačů v lokální síti, nikoliv však ze samotného firewallu (tj. počítače, na němž je *WinRoute* nainstalován)!

Komunikace mezi firewallem a Internetem musí být explixitně povolena samostatným pravidlem. Protože má počítač s *WinRoute* přímý přístup do Internetu, není třeba použít funkci překladu adres.

Zpřístupnění služby (mapování portů)

Mapování portů zpřístupňuje z Internetu službu běžící na počítači v lokální (zpravidla privátní) síti. Z pohledu klienta v Internetu tato služba běží na vnější IP adrese počítače s *WinRoute*. Komunikační pravidlo tedy musí být definováno následovně:

Zdroj Rozhraní připojené do Internetu (přes toto rozhraní budou přicházet požadavky klientů z Internetu).

Cíl Počítač s *WinRoute*, tj. speciální rozhraní *Firewall*.

Takto bude služba přístupná na všech adresách rozhraní připojeného do Internetu. Chcete-li službu zpřístupnit z konkrétní IP adresy, použijte volbu *Počítač* a zadejte požadovanou IP adresu.

Služba Služby, které mají být zpřístupněny. Službu lze vybrat ze seznamu předdefinovaných služeb (viz kapitola 8.3) nebo zadat přímo protokolem a číslem portu.

V tomto poli mohou být uvedeny všechny služby, které běží na jednom počítači. Pro zpřístupnění služeb z jiného počítače je třeba vytvořit nové komunikační pravidlo.

Akce Musí být nastavena na *Povolit* (jinak by byla komunikace blokována a mapování portů by nemělo žádný smysl).

Překlad V sekci *Překlad cílové adresy (mapování portů)* zvolte *Překládat na tuto IP adresu* a uveďte IP adresu počítače v lokální síti, kde služba běží.

Volbou *Překládat port na* je možné mapovat službu na jiný port, než na kterém je služba přístupná zvenčí.

Upozornění: V sekci *Překlad zdrojové adresy* musí být nastavena volba *Nepřekládat*! Kombinace překladu zdrojové i cílové adresy má význam pouze ve speciálních případech.

Poznámka: Pro správnou funkci mapování portů je nutné, aby počítač, na němž mapovaná služba běží, měl nastavenu výchozí bránu na počítač s *WinRoute*. Bez splnění této podmínky nebude mapování fungovat.

Umístění pravidla Pravidla pro mapování služeb jsou ve většině případů nezávislá na pravidlech pro překlad adres či omezení přístupu do Internetu i na sobě navzájem. Pro větší přehlednost doporučujeme umisťovat všechna tato pravidla buď na začátek, nebo na konec seznamu.

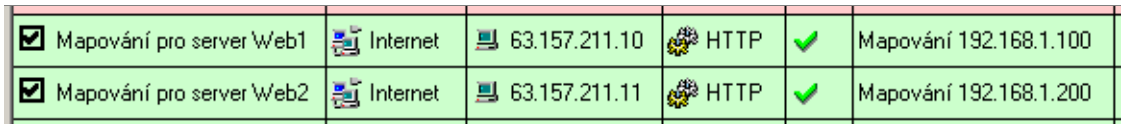
Existují-li pravidla omezující přístup k mapovaným službám, musí být vlastní pravidla pro mapování umístěna pod těmito pravidly.

Zpřístupnění služeb na různých IP adresách (multihoming)

Multihoming je označení pro situaci, kdy má síťové rozhraní připojené do Internetu přiřazeno více veřejných IP adres. Typickým požadavkem je, aby na těchto adresách byly nezávisle zpřístupněny různé služby.

Příklad: V lokální síti běží WWW server `web1` na počítači s IP adresou `192.168.1.100` a WWW server `web2` s IP adresou `192.168.1.200`. Rozhraní připojené do Internetu má přiřazeny veřejné IP adresy `63.157.211.10` a `63.157.211.11`. Server `web1` má být z Internetu dostupný na IP adrese `63.157.211.10`, server `web2` na IP adrese `63.157.211.11`.

Pro splnění těchto požadavků definujeme ve *WinRoute* dvě komunikační pravidla:



Zdroj Rozhraní připojené do Internetu (přes toto rozhraní budou přicházet požadavky klientů z Internetu).

Cíl Příslušná IP adresa rozhraní připojeného do Internetu (pro zadání jedné IP adresy slouží volba *Počítač*).

Služba Služba, která má být zpřístupněna (v případě WWW serveru služba *HTTP*).

Akce Musí být nastavena na *Povolit* (jinak by byla komunikace blokována a mapování portů by nemělo žádný smysl).

Překlad V sekci *Překlad cílové adresy (mapování portů)* zvolíme *Překládat na tuto IP adresu* a zadáme IP adresu odpovídajího WWW serveru (`web1`, resp. `web2`).

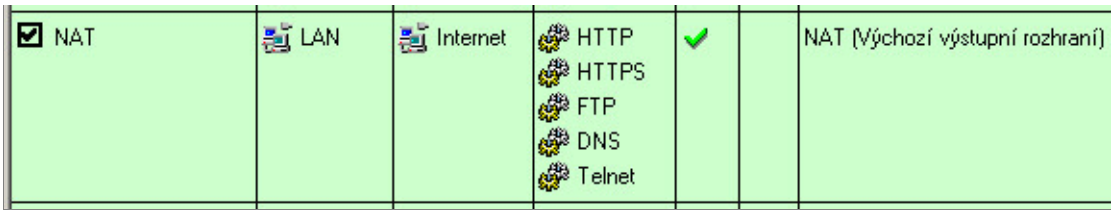
Omezení přístupu do Internetu

Velmi častým požadavkem je omezit přístup uživatelů z lokální sítě ke službám v Internetu. Omezení lze provést několika způsoby. V níže uvedených příkladech omezení zajišťuje přímo pravidlo pro překlad IP adres, a to specifikací podmínky, kdy má být překlad prováděn. Není třeba definovat žádné další pravidlo — implicitní pravidlo bude blokovat veškerou komunikaci, která těmto podmínkám nevyhoví.

Další způsoby omezování přístupu budou zmíněny v sekci *Výjimky* (viz níže).

Poznámka: Pravidla uvedená v těchto příkladech mohou být také použita, jestliže je *WinRoute* nasazen jako tzv. neutrální směrovač (tj. směrovač bez překladu IP adres) — pouze v položce *Překlad* nebude žádný překlad definován.

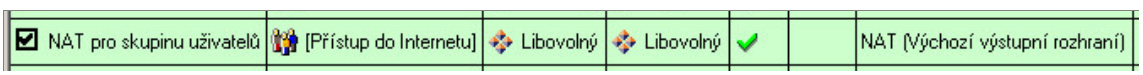
1. Povolení přístupu pouze k vybraným službám. V pravidle pro překlad IP adres uvedeme v položce *Služba* pouze služby, které mají být povoleny.



2. Omezení dle IP adres. Přístup k určitým službám (případně kompletní přístup do Internetu) bude povolen pouze z vybraných počítačů. V položce *Zdroj* definovaného pravidla uvedeme skupinu

   Poznámka: Definice pravidel tohoto typu je vhodná pouze v případě, že každý uživatel má svůj vlastní počítač (uživatelé se u počítačů nestřídají) a počítače mají přiřazeny statické IP adresy.

3. Omezení dle uživatelů. V tomto případě firewall kontroluje, zda z počítače, odkud komunikace přichází, je přihlášen určitý uživatel. Podle toho komunikaci povolí či zakáže.



   Nejjednodušší variantou tohoto omezení je pravidlo povolující přístup do Internetu pouze přihlášeným uživatelům. Internet tak bude dostupný všem uživatelům, kteří mají ve *WinRoute* uživatelský účet. Správce firewallu tak má detailní přehled o tom, kam kteří uživatelé přistupují a jaké služby využívají (anonymní přístup není možný).

Poznámka: Detailní informace o přihlašování uživatelů k firewallu naleznete v kapitole 7.2.

Výše uvedená pravidla lze také různým způsobem kombinovat — např. povolit skupině uživatelů přístup do Internetu pouze k vybraným službám.

Výjimky

Při omezování přístupu do Internetu může vzniknout požadavek, aby k určité službě byl povolen přístup pouze vybrané skupině uživatelů či IP adres. Všem ostatním uživatelům (resp. ze všech ostatních IP adres) má být přístup k této službě zakázán.

Jako příklad uvedeme povolení služby *Telnet* skupině uživatelů. Pro splnění tohoto požadavku definujeme dvě pravidla:

- První pravidlo povolí službu *Telnet* vybrané skupině uživatelů (resp. skupině IP adres apod.).
- Druhé pravidlo zakáže přístup k této službě všem ostatním uživatelům.

Kapitola 6

Filtrování obsahu

WinRoute poskytuje velmi rozsáhlé možnosti filtrování komunikace protokoly HTTP a FTP. Tyto protokoly patří k nejrozšířenějším a nejpoužívanějším protokolům v Internetu.

Mezi hlavní důvody filtrování obsahu HTTP a FTP patří:

- zamezit uživatelům v přístupu na nevhodné WWW stránky (např. stránky, které nesouvisejí s pracovní náplní zaměstnanců firmy)
- zamezit přenosu určitých typů souborů (např. nelegální obsah)
- zabránit či omezit šíření virů, červů a trojských koní

Podívejme se podrobněji na možnosti filtrování, které *WinRoute* nabízí. Jejich podrobný popis najdete v následujících kapitolách.

Protokol HTTP — filtrování WWW stránek:

- omezování přístupu podle URL (resp. podřetězce obsaženého v URL)
- blokování určitých prvků HTML (např. skripty, objekty ActiveX apod.)
- filtrování na základě ohodnocení systémem *Cobion Orange Filter* (celosvětová databáze klasifikací WWW stránek)
- omezování přístupu na stránky obsahující určitá slova
- antivirová kontrola stahovaných objektů

Protokol FTP — kontrola přístupu na FTP servery:

- úplný zákaz přístupu na zadané FTP servery
- omezení podle jména souboru
- omezení přenosu souborů na jeden směr (např. pouze download)

- blokování určitých příkazů protokolu FTP
- antivirová kontrola přenášených souborů

Kdy filtrování obsahu funguje?

Pro činnost výše popsaného filtrování obsahu musí být splněny dvě základní podmínky:

1. Komunikace musí být obsluhována příslušným inspekčním modulem.

   Poznámka: Potřebný inspekční modul je aktivován automaticky, pokud není komunikačními pravidly explicitně určeno, že nemá být pro danou komunikaci použit. Podrobnosti najdete v kapitole 5.2.

2. Spojení nesmí být šifrováno. Komunikaci zabezpečenou SSL (tj. protokoly HTTPS a FTPS) není možné sledovat. V tomto případě lze pouze blokovat přístup na konkrétní servery komunikačními pravidly (viz kapitola 5.2).

3. Protokol FTP nelze filtrovat při použití zabezpečeného přihlášení (*SASO*).

Poznámka: WinRoute nabízí pouze nástroje pro filtrování a omezování přístupu. Rozhodnutí, jaké WWW stránky a typy souborů mají být blokovány, musí učinit správce *WinRoute* (případně jiná kompetentní osoba).

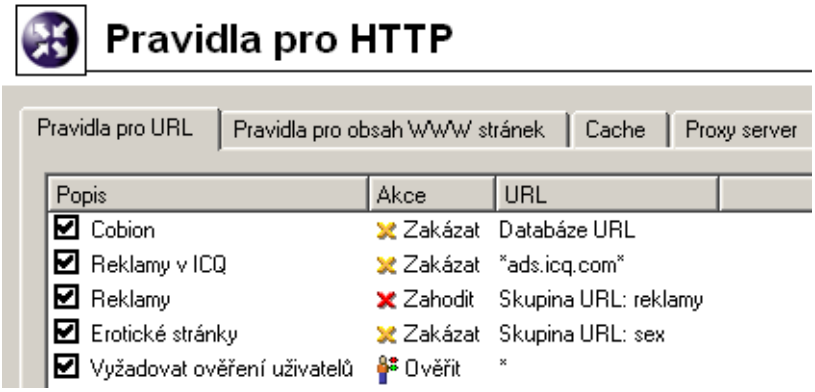
6.1 Pravidla pro URL

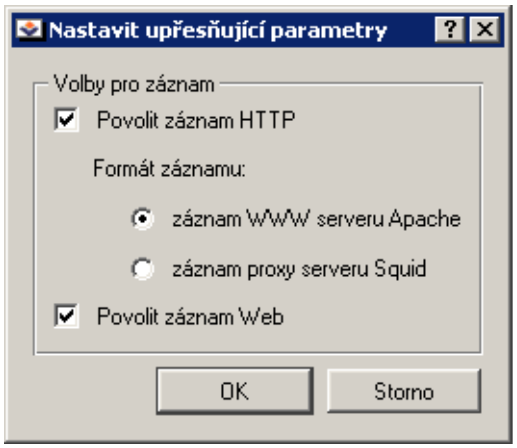
Tato pravidla umožňují omezit přístup vybraných uživatelů k WWW stránkám, jejichž URL vyhovují určitým kritériím. Další důležitou funkcí pravidel pro URL je možnost vyžádat ověření uživatele na firewallu automatickým přesměrováním prohlížeče na přihlašovací stránku (viz kapitola 7.2). Při přístupu na stránku, která vyžaduje ověření, pak uživatel nemusí „ručně“ otevírat přihlašovací stránku a poté zadávat znovu URL požadované stránky.

Pravidla pro URL se definují v sekci *Konfigurace / Filtrování obsahu / Pravidla pro HTTP*, záložka *Pravidla pro URL*.

Pravidla v této sekci jsou vždy procházena shora dolů (pořadí lze upravit tlačítky se šipkami na pravé straně okna). Vyhodnocování se zastaví na prvním pravidle, kterému dané URL vyhoví. Pokud URL nevyhoví žádnému pravidlu, je přístup na stránku povolen (implicitně vše povoleno).

Tlačítkem *Upřesnění* lze zakázat/povolit HTTP a Web záznamy (logy). U položky *Povolit záznam HTTP* může být vybrán i formát záznamu (WWW serveru Apache nebo proxy serveru Squid).





Poznámka: Výchozí instalace *WinRoute* obsahuje několik předdefinovaných pravidel pro URL. Tato pravidla jsou ve výchozím nastavení „vypnuta“. Správce *WinRoute* je může použít, případně upravit dle vlastního uvážení.

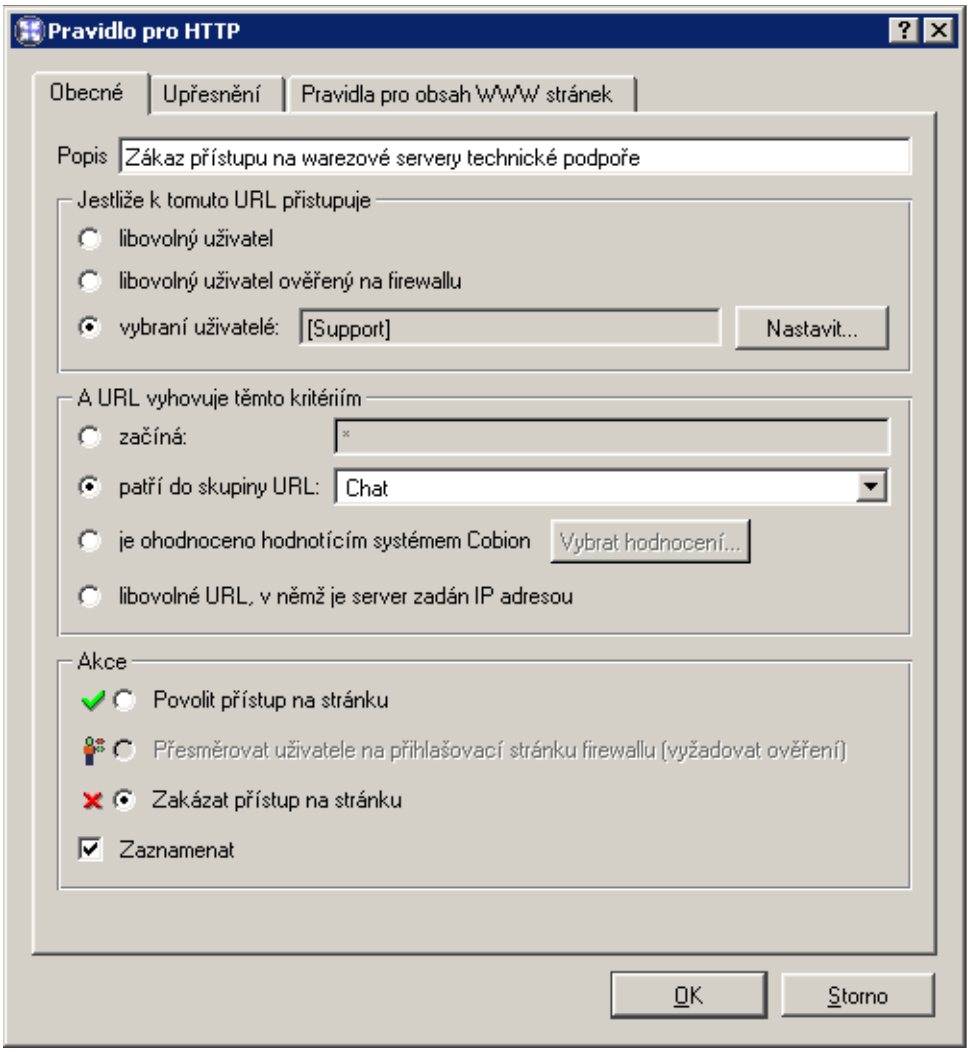
Tlačítko *Přidat* otevírá dialog pro definici nového pravidla.

Záložka *Obecné* slouží k nastavení základních podmínek a akcí, které mají být při jejich splnění provedeny.

Popis Slovní popis funkce pravidla (pro snazší orientaci správce *WinRoute*).

Jestliže k tomuto URL přistupuje Volba, pro které uživatele bude toto pravidlo platit:

- *libovolný uživatel* — pro všechny uživatele (bez ohledu na to, zda jsou na firewallu ověřeni či nikoliv)
- *libovolný uživatel ověřený na firewallu* — pro všechny uživatele, kteří jsou přihlášeni
- *vybraní uživatelé* — pro vybrané uživatele a/nebo skupiny uživatelů.



Tlačítko *Nastavit* otevírá dialog pro výběr uživatelů a skupin (přidržením kláves *Ctrl* a *Shift* můžete vybrat více uživatelů / skupin současně).

Poznámka: Povolení nebo omezení vztahující se na vybrané uživatele (případně na všechny přihlášené uživatele) má smysl pouze v kombinaci s pravidlem zakazujícím přístup všem uživatelům nebo vyžadujícím ověření uživatele, který není dosud přihlášen (podrobnosti viz dále).

A URL vyhovuje těmto kritériím Specifikace URL (resp. množiny URL), pro které má toto pravidlo platit:

- *začíná* — v této položce může být uvedeno kompletní URL

(např. `www.kerio.cz/index.html`), podřetězec URL s použitím hvězdičkové konvence (např. `*.ker?o.cz*`) nebo jméno serveru (např. `www.kerio.cz`). Jméno serveru má význam libovolného URL na daném serveru (`www.kerio.com/*`).

- *patří do skupiny URL* — výběr skupiny URL (viz kapitola 8.4), které má URL vyhovovat
- *je ohodnoceno hodnotícím systémem Cobion* — pravidlo bude platit pro všechny stránky, které systém *Cobion Orange Filter* zařadí do některé z vybraných kategorií.

  Tlačítko *Vybrat hodnocení...* otevírá dialog pro výběr kategorií systému *Cobion Orange Filter*. Podrobnější informace naleznete v kapitole 6.3.
- *libovolné URL, v němž je server zadán IP adresou* — takto musí být zadáno URL stránky či souboru na WWW serveru, který nemá záznam v DNS. Toto je charakteristické např. pro servery nabízející ke stažení soubory s nelegálním obsahem.

  Upozornění: Není-li zakázán přístup na servery zadané IP adresou, mohou takto uživatelé obcházet pravidla pro URL, ve kterých jsou servery uváděny jménem!

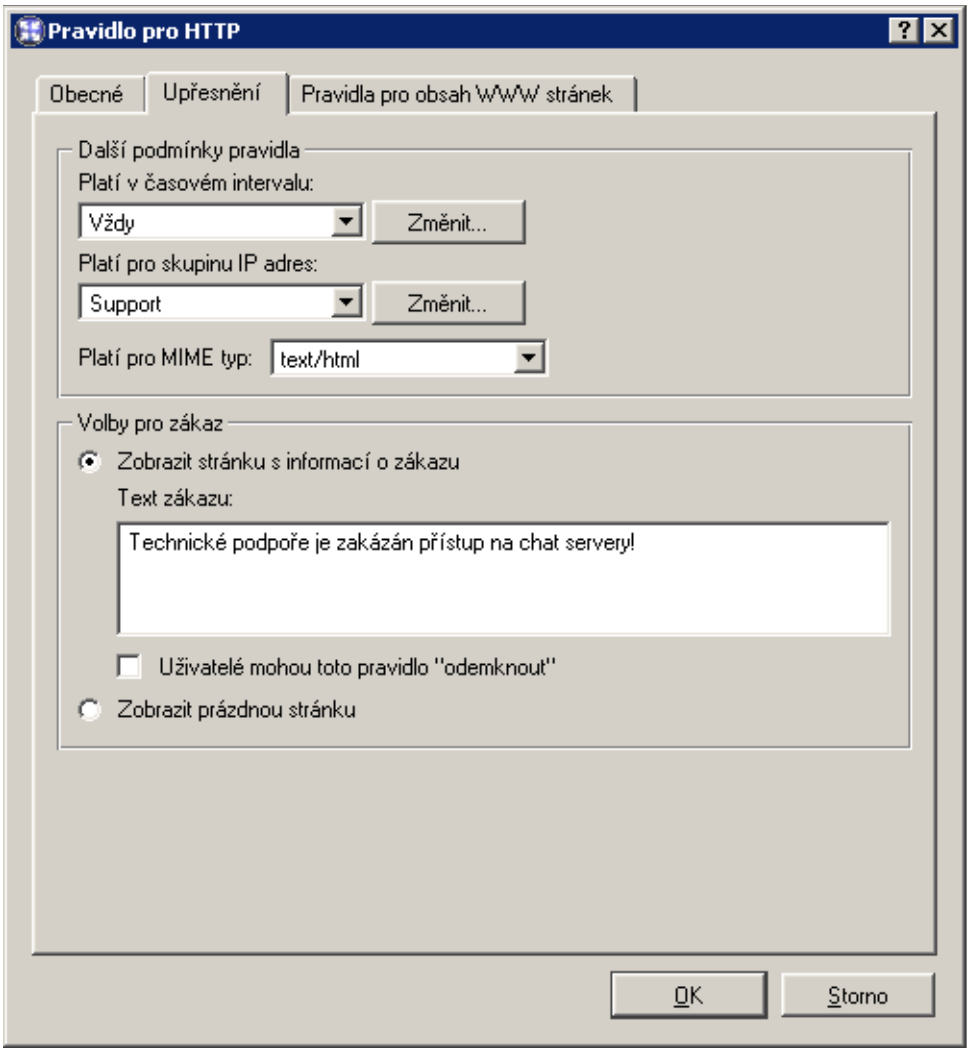
Akce Volba akce, která bude provedena, jestliže jsou splněny podmínky pro uživatele a URL:

- *Povolit přístup na stránku*
- *Přesměrovat uživatele na přihlašovací stránku (vyžadovat ověření)* — není-li dosud uživatel na firewallu ověřen, bude *WinRoute* vyžadovat přihlášení. Přistupuje-li uživatel k WWW stránkám přes proxy server ve *WinRoute*, zobrazí jeho prohlížeč dialog pro zadání uživatelského jména a hesla. V případě přímého přístupu je prohlížeč automaticky přesměrován na přihlašovací stránku (viz kapitola 7.2) a po úspěšném přihlášení na požadovanou stránku.

  Na uživatele, kteří jsou již přihlášeni, nebude mít toto pravidlo žádný vliv.
- *Zakázat přístup na stránku* — požadovaná stránka bude blokována. Uživateli se zobrazí stránka s informací o zákazu nebo prázdná stránka (dle nastavení v záložce *Upřesnění* — viz dále).

Zaškrtnutím volby *Zaznamenat* budou všechny přístupy na stránky, které vyhověly tomuto pravidlu, zaznamenávány do záznamu *Filter* (viz kapitola 12.4).

V záložce *Upřesnění* obsahuje další podmínky, za kterých má pravidlo platit, a volby pro zakázané stránky.



Platí v časovém intervalu Výběr časového intervalu platnosti pravidla (mimo tento interval je pravidlo neaktivní). Tlačítko *Změnit* otevírá dialog pro úpravu časových intervalů (podrobnosti viz kapitola 8.2).

Platí pro skupinu IP adres Výběr skupiny IP adres, pro kterou bude toto pravidlo platit (jedná se o zdrojové IP adresy, tedy adresy klientů). Speciální volba *Libovolná* znamená, že pravidlo nebude závislé na IP adrese klienta.

Tlačítko *Změnit* otevírá dialog pro úpravu skupin IP adres (podrobnosti viz kapitola 8.1).

Platí pro MIME typ Omezení platnosti pravidla pouze na objekty určitého MIME typu (např.: `text/html` — HTML dokumenty, `image/jpeg` — obrázky typu JPEG apod.).

V této položce můžete vybrat některý z předdefinovaných MIME typů nebo zadat vlastní. Při definici MIME typu lze použít hvězdičku pro specifikaci libovolného subtypu (např. `image/*`). Samotná hvězdička znamená libovolný MIME typ — pravidlo bude nezávislé na MIME typu objektu.

Volby pro zákaz Upřesňující nastavení pro zakázané stránky. Jestliže se uživatel pokusí otevřít stránku, na kterou je tímto pravidlem zakázán přístup, pak *WinRoute* místo této stránky zobrazí:

- stránku s informací o zakázaném přístupu — uživatel se dozví, že požadovaná stránka je blokována firewallem. Tato stránka může být doplněna vysvětlením zákazu (položka *Text zákazu*).

  Bude-li zaškrtnuta volba *Uživatelé mohou toto pravidlo odemknout*, pak se přihlášeným uživatelům na stránce s informací o zákazu zobrazí tlačítko *Odemknout*. Stisknutím tohoto tlačítka si uživatel může vynutit povolení přístupu na požadovanou stránku, přestože jej pravidlo pro URL zakazuje. Odemknutí stránky je časově omezeno (standardně 10 minut). Každý uživatel může odemknout jen omezený počet zakazujících pravidel (maximálně 10 pravidel současně). Všechny požadavky na odemknutí se zaznamenávají do záznamu *Filter* (viz kapitola 12.4).

  Poznámky:

  1. Odemykat pravidla smějí pouze uživatelé, kteří jsou na firewallu přihlášeni.

  2. Při jakékoliv změně v pravidlech pro URL se všechna odemknutí ihned ruší.

- prázdnou stránku — uživatel nezíská žádné informace o tom, proč se požadovaná stránka nezobrazila (nedozví se ani o existenci *WinRoute*)

Nové pravidlo bude přidáno pod pravidlo, které bylo označené před stisknutím tlačítka *Přidat*. Šipkovými tlačítky na pravé straně okna přesuňte vytvořené pravidlo na požadované místo.

Zaškrtávací pole vedle popisu pravidla slouží k jeho „vypnutí“ — pravidlo můžete dočasně vyřadit bez nutnosti jej odstraňovat a poté znovu přidávat.

Poznámka: Přístup k URL, pro které neexistuje odpovídající pravidlo, je povolen (implicitně vše povoleno). Chceme-li povolit přístup pouze k omezené skupině stránek a všechny ostatní stránky blokovat, je třeba na konec seznamu umístit pravidlo zakazující přístup k libovolnému URL.

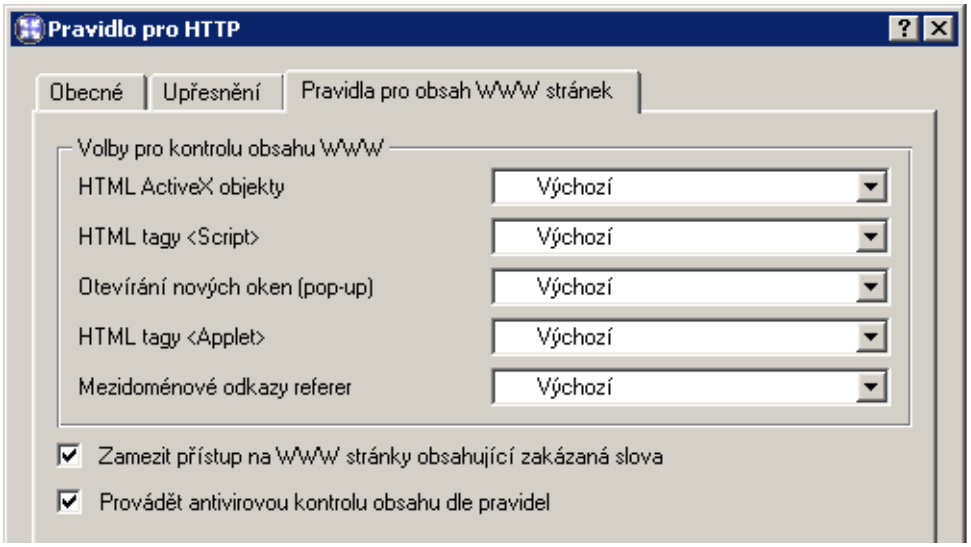
Záložka *Pravidla pro obsah WWW stránek* umožňuje zpřesnit povolení přístupu na WWW stránky.

Možnosti jsou:

Povolit Volba povolena.

Zakázat Volba zakázána.

Výchozí Pro volbu bude platit výchozí hodnota nastavená každému uživatelskému účtu.



HTML ActiveX objekty Prvky Microsoft ActiveX (bezpečnostní problémy v implementaci této technologie umožňují např. spouštění aplikací na klientském počítači).

HTML tagy <Script> HTML tagy `<script>` — příkazy jazyků JavaScript, VBScript atd.

Otevírání nových oken Automatické otevírání nových oken prohlížeče — typicky reklamy.

Je-li tato volba vypnuta, pak *WinRoute* blokuje ve skriptech metodu `window.open()`.

HTML tagy <Applet> HTML tagy `<applet>` (*Java Applet*)

Mezidoménové odkazy referer

Položka `Referer` v HTTP hlavičce.

Tato položka obsahuje URL stránky, z níž klient na danou stránku přešel. Po vypnutí volby *Povolit mezidoménové odkazy referer* bude položka `Referer` blokována v případě, že obsahuje jiné jméno serveru než aktuální HTTP požadavek.

Blokování mezidoménových odkazů v položkách `Referer` má význam pro ochranu soukromí uživatele (položka `Referer` může být sledována pro zjištění, jaké stránky uživatel navštěvuje).

Zamezit přístup na WWW stránky ... Pokud volba obsahuje zakázaná slova definovaná v sekci *Konfigurace / Pravidla pro HTTP* (více v kapitole 6.4), lze zaškrtnutím zamezit uživateli přístup na příslušné WWW stránky.

Provádět antivirovou kontrolu obsahu dle pravidel Po zaškrtnutí volby bude prováděna antivirová kontrola podle pravidel (kapitola 6.6).

Vyžádání ověření uživatelů na firewallu

Pravidla pro URL lze také využít pro vyžádání ověření uživatelů na firewallu. Při přístupu na určitou stránku může být prohlížeč automaticky přesměrován na přihlašovací stránku, a po úspěšném přihlášení zobrazí požadovanou stránku. Ověření uživatele má význam nejen pro řízení přístupu uživatelů na WWW stránky (případně k jiným službám), ale také pro sledování aktivit uživatelů (viz kapitola 12) — využívání Internetu není anonymní.

Doporučeným postupem je vytvořit pravidlo, které bude vyžadovat ověření uživatele při přístupu k libovolnému URL.

Ověření uživatele bude vyžadováno v případě, že není k firewallu dosud přihlášen. Na přihlášené uživatele se toto pravidlo nevztahuje.

Toto pravidlo může být kombinováno s libovolnými pravidly povolujícími či zakazujícími přístup k určitým URL vybraným uživatelům (případně zakazujícími přístup všem uživatelům).

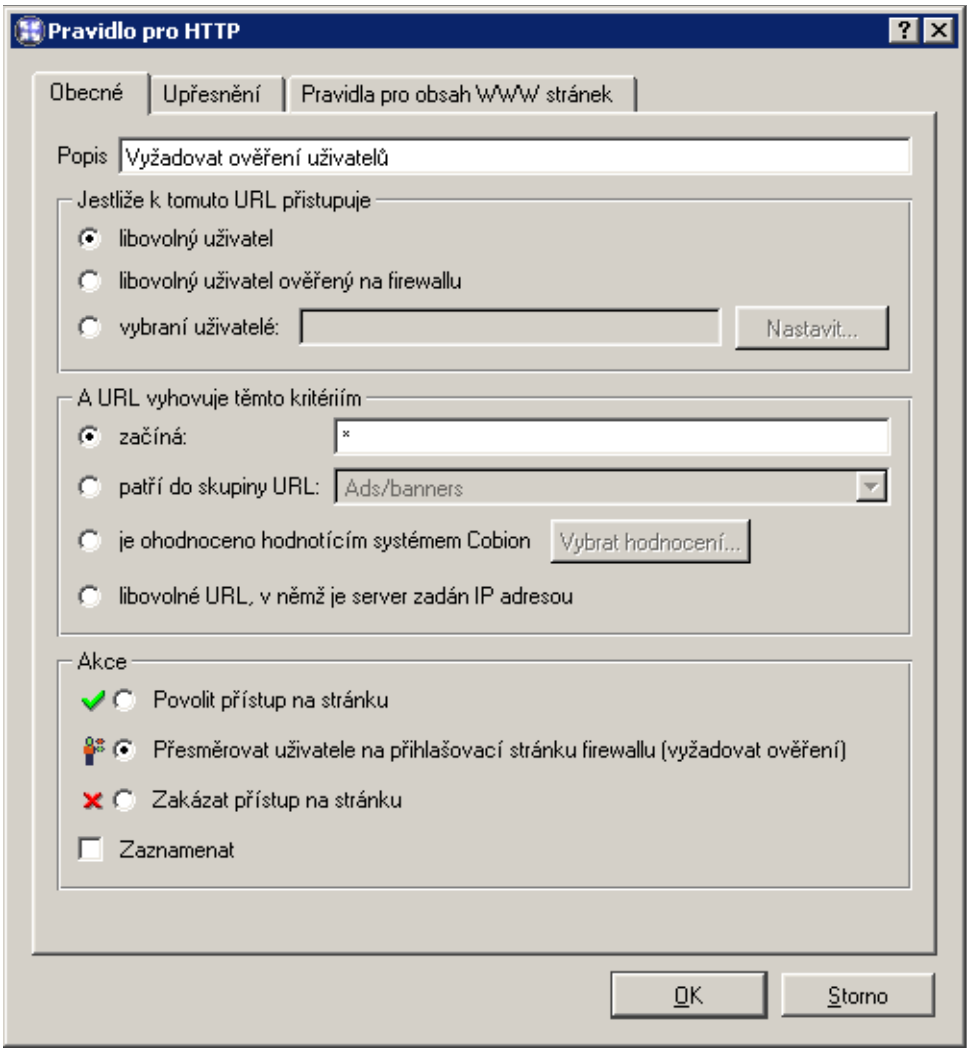
Poznámky:

1. Možnost vyžádat ověření uživatele neexistuje u žádné jiné služby než *HTTP*. Bude-li např. komunikačními pravidly (viz kapitola 5.2) omezen přístup ke službě *Telnet* dle uživatelů, pak bude muset každý uživatel nejprve otevřít přihlašovací stránku (viz kapitola 7.2), přihlásit se a teprve potom se bude moci připojit programem *Telnet* na požadovaný server.

2. Nefunguje-li aktualizace antivirového programu (viz kapitola 6.6), může to být způsobeno tím, že *WinRoute* vyžaduje ověření uživatele a automaticky přesměrovává klienta na přihlašovací stránku. Tuto situaci lze řešit dvěma způsoby:

   - vytvořit pravidlo povolující přístup k WWW serveru, odkud se aktualizace stahují, bez nutnosti přihlášení uživatele

   - pokud to antivirus umožňuje, nastavit používání proxy serveru (viz kapitola 4.4) a zadat uživatelské jméno a heslo pro ověření



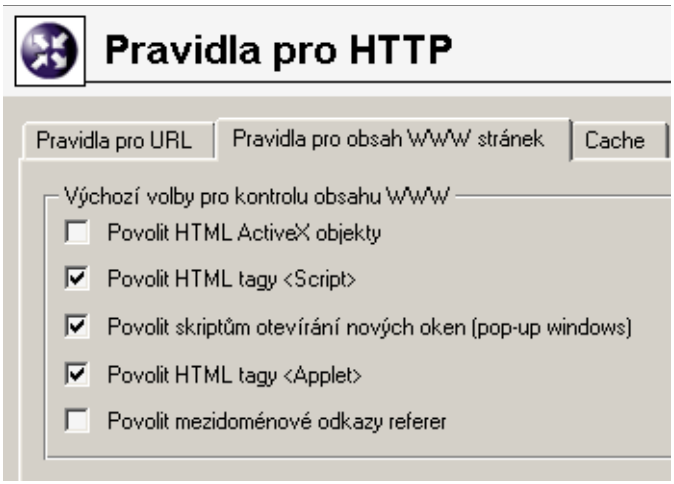
6.2 Pravidla pro obsah WWW stránek

WinRoute umožňuje blokovat určité prvky v HTML stránkách. Blokování funguje globálně pro HTTP komunikaci, kterou *WinRoute* obsluhuje.

Filtrování obsahu WWW stránek se nastavuje v sekci *Konfigurace / Filtrování obsahu / Pravidla pro HTTP*, záložka *Pravidla pro obsah WWW stránek*.

Povolit HTML ActiveX objekty Prvky Microsoft ActiveX (bezpečnostní problémy v implementaci této technologie umožňují např. spouštění aplikací na klientském počítači).

Povolit HTML tagy <Script> HTML tagy `<script>` — příkazy jazyků JavaScript, VBScript atd.



Povolit skriptům otevírání nových oken Automatické otevírání nových oken prohlížeče — typicky reklamy.

Je-li tato volba vypnuta, pak *WinRoute* blokuje ve skriptech metodu `window.open()`.

Povolit HTML tagy <Applet> HTML tagy `<applet>` (*Java Applet*)

Povolit mezidoménové odkazy referer Položka `Referer` v HTTP hlavičce.

Tato položka obsahuje URL stránky, z níž klient na danou stránku přešel. Po vypnutí volby *Povolit mezidoménové odkazy referer* bude položka `Referer` blokována v případě, že obsahuje jiné jméno serveru než aktuální HTTP požadavek.

Blokování mezidoménových odkazů v položkách `Referer` má význam pro ochranu soukromí uživatele (položka `Referer` může být sledována pro zjištění, jaké stránky uživatel navštěvuje).

Poznámka: Nastavení v záložce *Pravidla pro obsah WWW stránek* platí pro nepřihlášené uživatele. Každý přihlášený uživatel si může nastavení filtrování upravit na stránce osobních preferencí (viz kapitola 7.3). Nemá-li uživatel právo *přejít pravidla pro obsah WWW stránek* (viz kapitola 9.1), smí nastavení pouze zpřísnit — nemůže povolit HTML prvek, který je globálně zakázán.

6.3 Systém hodnocení obsahu Cobion Orange Filter

Systém *Cobion Orange Filter*, který je integrován ve *WinRoute*, slouží k hodnocení obsahu WWW stránek. Každá stránka je tímto systémem zařazena do některé z předdefinovaných kategorií. Na základě této klasifikace k ní může být určitým uživatelům povolen či zakázán přístup.

Základem systému *Cobion Orange Filter* je celosvětová dynamická databáze, která obsahuje URL stránek a jejich klasifikace. Tuto databázi udržují speciální servery, které provádějí hodnocení jednotlivých stránek. Přistupuje-li uživatel k určité stránce, modul *Cobion Orange Filter* ve *WinRoute* se dotáže databázového serveru na klasifikaci URL této stránky a podle klasifikace rozhodne, zda má přístup na stránku povolit či zakázat. Pro urychlení vyhodnocování jednotlivých URL mohou být získané odpovědi uloženy do lokální vyrovnávací paměti (cache), kde jsou po určitou dobu uchovány.

Poznámka: Systém *Cobion Orange Filter* byl vyvinut a testován zejména pro stránky v anglickém jazyce. Úspěšnost klasifikace stránek v jiných jazycích (např. v češtině) je nižší — cca 70 %.

Použití systému Cobion Orange Filter

Hodnotící systém *Cobion Orange Filter* se aktivuje vždy, když *WinRoute* zpracovává pravidlo pro URL, ve kterém je jako podmínka zadána klasifikace stránky do určitých kategorií. Jako příklad uvedeme pravidlo zakazující všem uživatelům přístup na stránky s nabídkou pracovních míst.

V sekci *Konfigurace / Filtrování obsahu / Pravidla pro HTTP*, záložka *Pravidla pro URL*, definujeme následující pravidlo:

Klíčovým parametrem je volba *je ohodnoceno hodnotícím systémem Cobion*. URL každé navštívené stránky bude klasifikováno systémem *Cobion Orange Filter*, a bude-li zařazeno do některé z vybraných kategorií, pak *WinRoute* zakáže přístup na tuto stránku.

Tlačítkem *Vybrat hodnocení* otevřeme dialog pro výběr kategorií systému *Cobion Orange Filter* a zvolíme kategorii

Job Search (stránky s nabídkami pracovních míst).

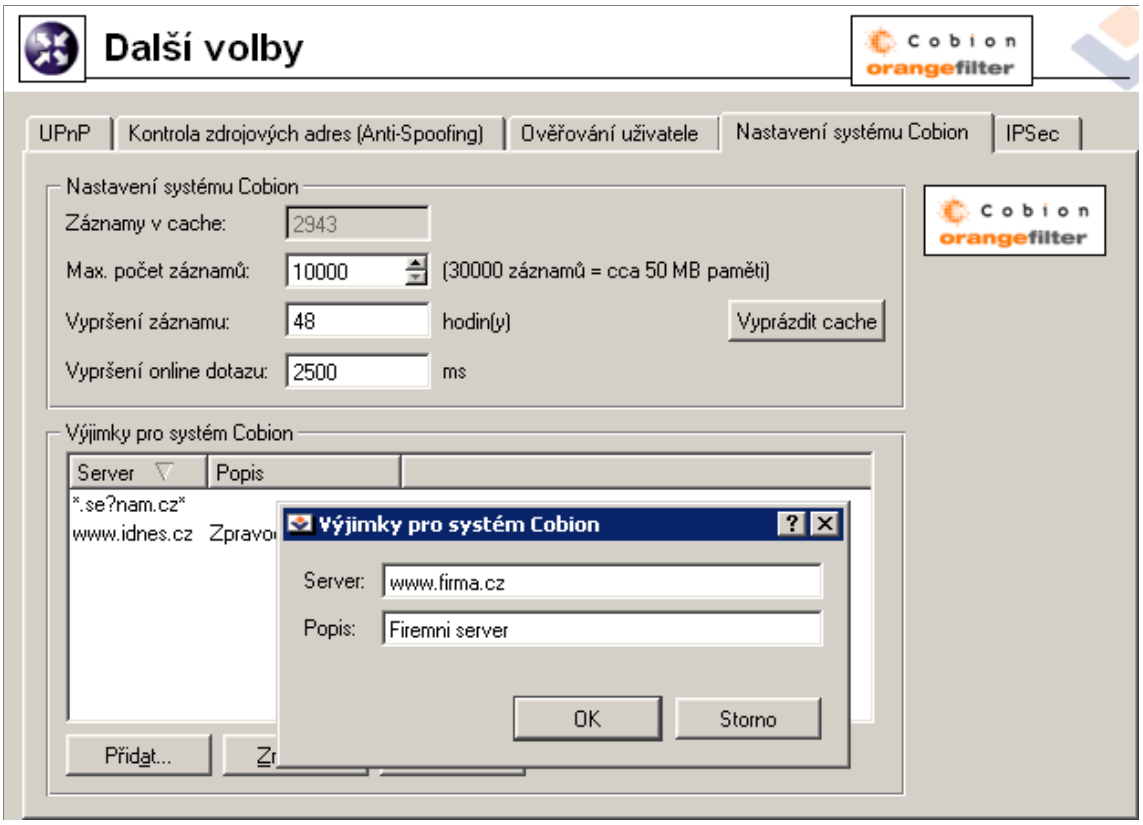
Poznámka: V pravidlech používajících systém *Cobion Orange Filter* je vhodné povolit odemknutí (záložka *Upřesnění*, volba *Uživatelé mohou toto pravidlo "odemknout"*) — pro případ, že bude stránka blokována z důvodu nesprávné klasifikace.

Nastavení parametrů systému Cobion Orange Filter

K nastavení upřesňujících parametrů systému *Cobion Orange Filter* slouží záložka *Nastavení systému Cobion* v sekci *Konfigurace / Další volby*.

V poli *URL cache* můžete povolit či zakázat vyrovnávací paměť (cache) databáze klasifikací URL a nastavit její parametry.

Povoleno Tato volba zapíná URL cache. Použití URL cache je výhodné zejména při větším počtu uživatelů a/nebo pomalém internetovém připojení.



Upozornění: Cache není aktivována ihned, ale až po restartu *WinRoute Firewall Engine*.

Adresář Adresář (včetně kompletní cesty) pro URL cache. Pokud tento adresář neexistuje, *WinRoute* jej automaticky vytvoří.

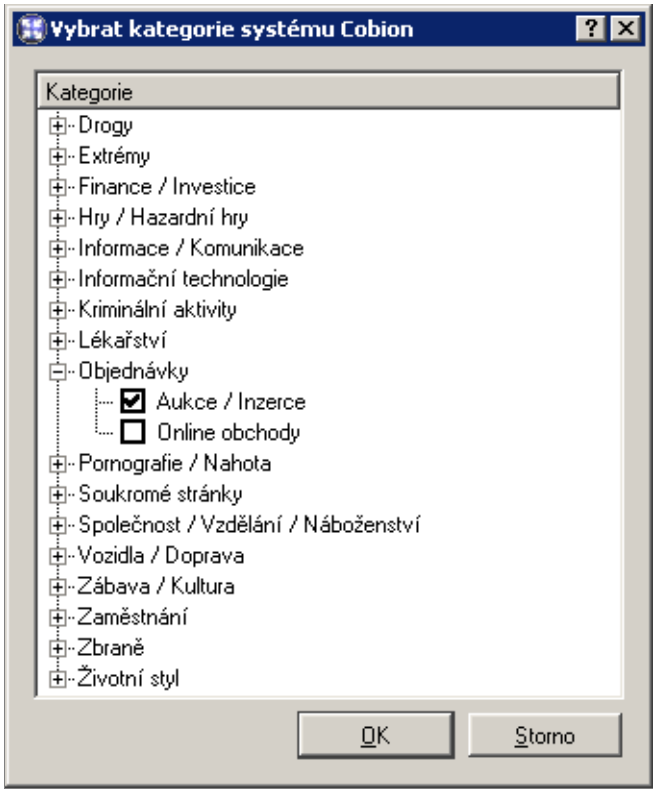
Záznamy v cache Aktuální počet záznamů uložených v URL cache

Max. počet záznamů Maximální počet záznamů databáze, které mohou být do cache uloženy. Tato hodnota ovlivňuje velikost potřebného diskového prostoru a rychlost prohledávání cache.

Vypršení záznamu v cache Maximální doba uchování záznamu v cache (po této době je záznam považován za neplatný). Databáze systému *Cobion Orange Filter* má dynamickou povahu, protože obsah WWW stránek (a tím i jejich klasifikace) se může v čase měnit.

Vyprázdnit cache Stisknutím tohoto tlačítka smažeme všechny záznamy uložené v URL cache.

Vypršení online dotazu Maximální doba čekání na odpověď od databázového serveru. Pokud se nepodaří získat odpověď do této doby, je stránka prohlášena za neklasi-



fikovatelnou a nevyhoví pravidlu, ve kterém je hodnocení systémem *Cobion Orange Filter* použito.

Poznámka: Informace o neklasifikovatelnosti stránky se neukládá do cache — při dalším přístupu na takovou stránku se *WinRoute* pokusí dotázat znovu.

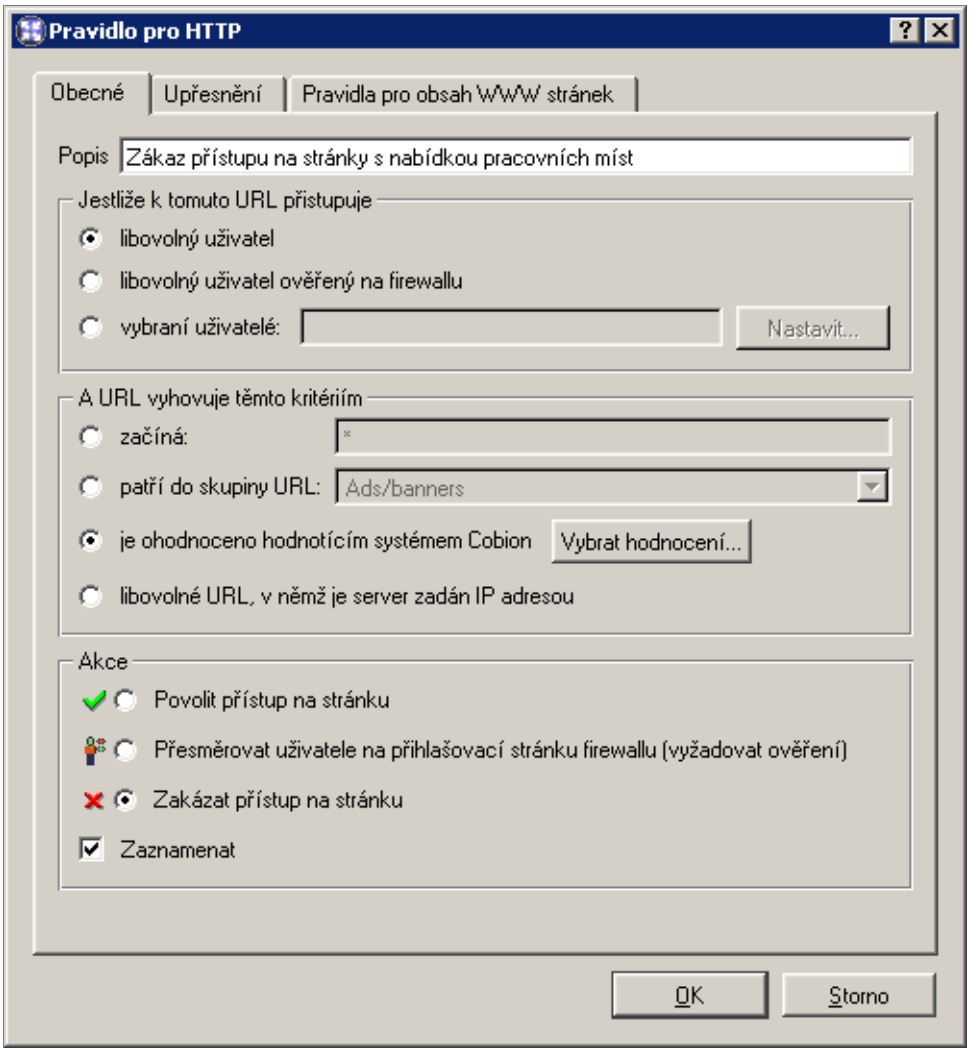
Výjimky pro systém Cobion Servery, které budou zadány v této části dialogu, nebudou kategorizovány systémem *Cobion Orange Filter*. Tlačítkem *Přidat* lze zadat novou položku (server).

Server Jméno serveru lze zadat několika způsoby (např. `www.seznam.cz/index.html`), podřetězec URL s použitím hvězdičkové konvence (např. `*.sez?am.cz*`) nebo jméno serveru (např. `www.seznam.cz`). Jméno serveru má význam libovolného URL na daném serveru (`www.seznam.com/*`).

Popis Popis slouží k lepší orientaci, není nutné jej vyplňovat.

6.4 Filtrování dle výskytu slov

WinRoute může filtrovat WWW stránky podle výskytu nežádoucích slov. Filtrování dle výskytu slov funguje globálně pro HTTP komunikaci, kterou obsluhuje inspekční modul

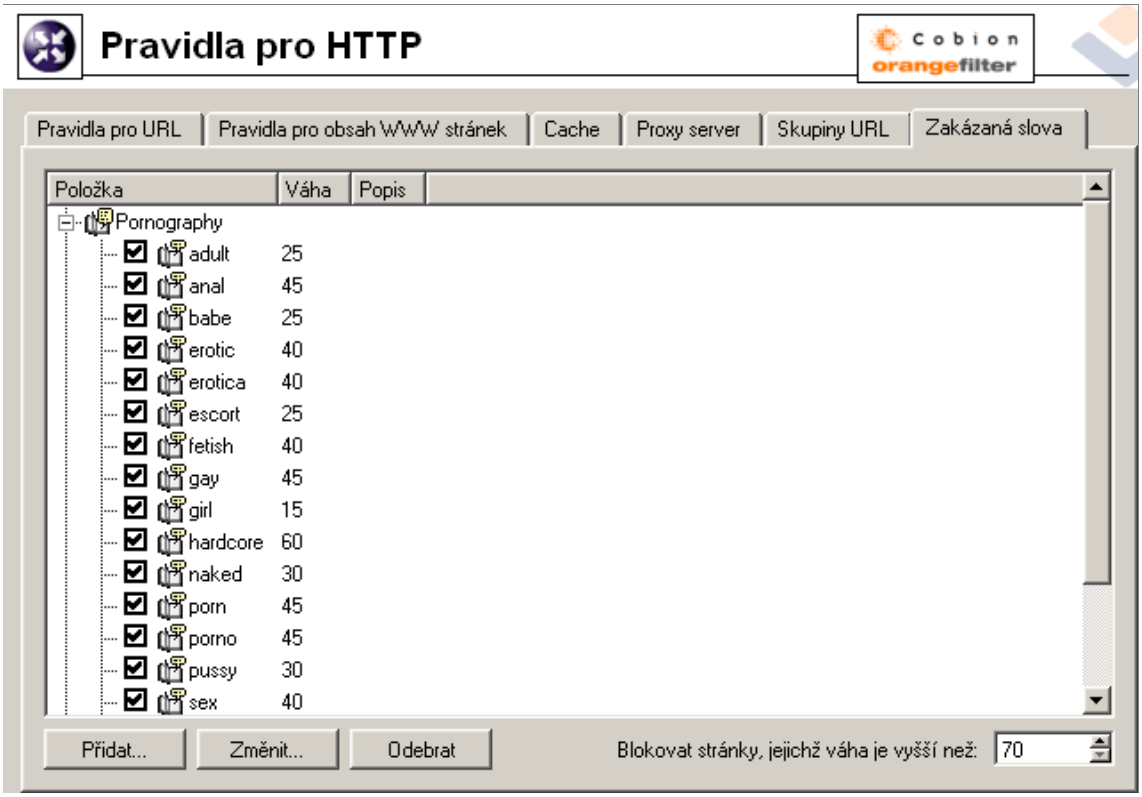


protokolu HTTP. Filtrování dle výskytu slov se provádí po aplikaci pravidel pro URL (pouze je-li přístup na danou stránku povolen).

Princip filtrování: každému nežádoucímu slovu je přiřazena určitá hodnota, tzv. váha (celé kladné číslo). Váhy jednotlivých slov nalezených na stránce se sčítají (váha každého slova je započítána pouze jednou, bez ohledu na počet jeho výskytů na stránce). Jestliže celková váha stránky překročí nastavenou hodnotu, stránka je blokována.

Jednotlivá slova se pro přehlednost řadí do skupin. Zařazení do skupiny nemá žádný vliv na filtrování — vždy se testují všechna slova ze všech skupin.

K definici skupin slov slouží záložka *Skupiny slov* v sekci *Konfigurace / Filtrování obsahu / Pravidla pro HTTP*.



Jednotlivé skupiny a v nich obsažená slova se zobrazují v podobě stromu. Zaškrtávací pole vlevo vedle každého slova umožňuje „vypnutí“ slova (dočasné vyřazení slova bez nutnosti jej odstraňovat a poté znovu přidávat).

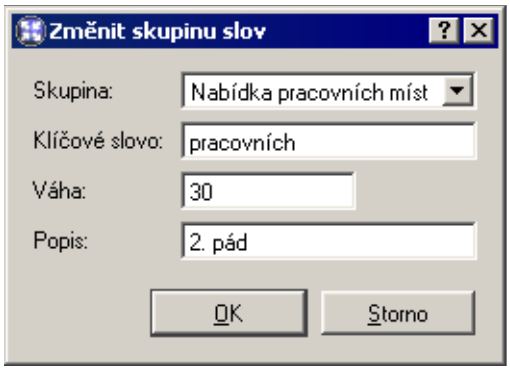
Poznámka: Ve výchozí instalaci *WinRoute* jsou předdefinovány tyto skupiny slov:

- *Pornography* — slova, která se typicky vyskytují na stránkách s erotickou tématikou
- *Warez* — slova, která obvykle obsahují stránky nabízející ke stažení nelegální software, generátory licenčních klíčů apod.

Všechna slova v předdefinovaných skupinách jsou ve výchozím nastavení „vypnuta“. Správce *WinRoute* je může použít a upravit jejich váhu dle vlastního uvážení.

Blokovat stránky, jejichž váha je vyšší než Prahová hodnota celkové váhy stránky (tj. součtu vah všech nalezených nežádoucích slov na stránce). Je-li celková váha stránky větší než zadaná hodnota, přístup na tuto stránku bude blokován (váha každého slova je započtena pouze jednou, bez ohledu na počet výskytů slova na stránce).

Tlačítko *Přidat* otevírá dialog pro přidání nového slova do skupiny nebo vytvoření nové skupiny.



Skupina Výběr skupiny, do které má být slovo zařazeno. Do této položky můžete také zadat název dosud neexistující skupiny — tím dojde k vytvoření nové skupiny.

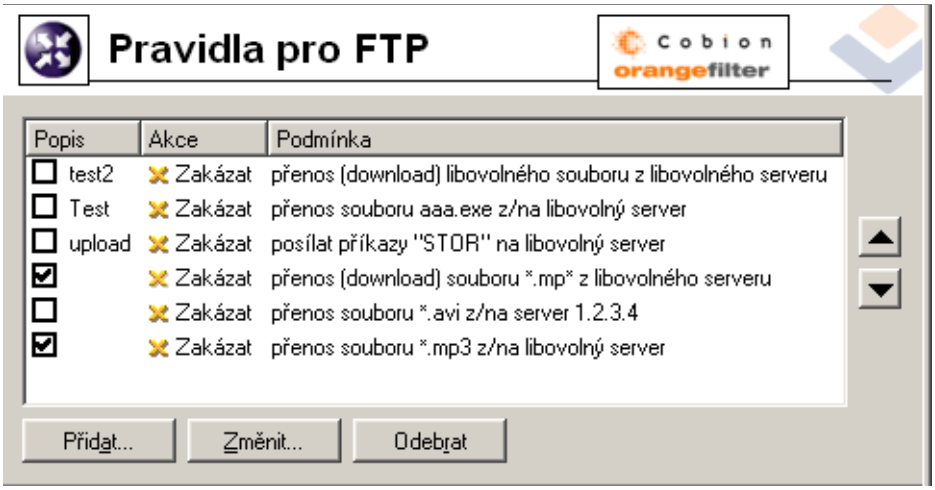
Klíčové slovo Nežádoucí slovo, které má být na stránce vyhledáno

Váha Váha slova (míra vlivu slova na blokaci přístupu na stránku)

Popis Libovolný textový komentář (pro přehlednost)

6.5 Filtrování protokolu FTP

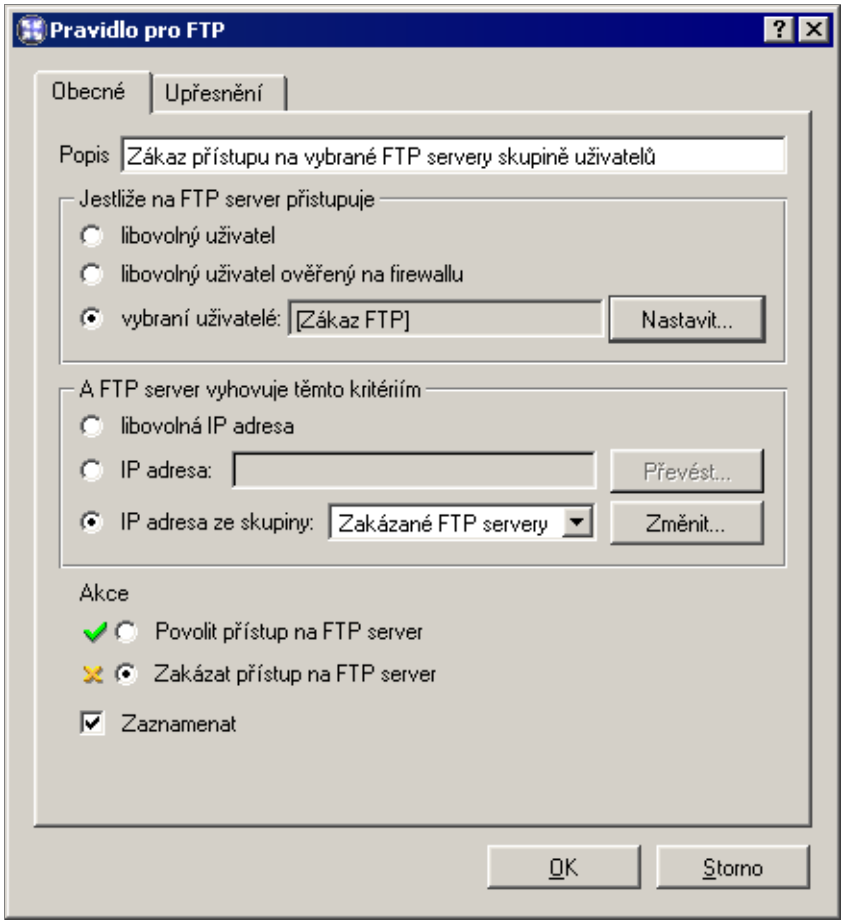
Pravidla pro přístup na FTP servery se nastavují v sekci *Konfigurace / Filtrování obsahu / Pravidla pro FTP*.



Pravidla v této sekci jsou vždy procházena shora dolů (pořadí lze upravit tlačítky se šipkami na pravé straně okna). Vyhodnocování se zastaví na prvním pravidle, kterému FTP požadavek vyhoví. Pokud požadavek nevyhoví žádnému pravidlu, je přístup na FTP server povolen (implicitně vše povoleno).

Poznámka: Výchozí instalace *WinRoute* obsahuje několik předdefinovaných pravidel pro FTP. Tato pravidla jsou ve výchozím nastavení „vypnuta“. Správce *WinRoute* je může použít, případně upravit dle vlastního uvážení.

Tlačítko *Přidat* otevírá dialog pro definici nového pravidla pro FTP.



Záložka *Obecné* slouží k nastavení základních podmínek a akcí, které mají být při jejich splnění provedeny.

Popis Slovní popis funkce pravidla (pro snazší orientaci správce *WinRoute*).

Jestliže na FTP server přistupuje Volba, pro které uživatele bude toto pravidlo platit:

- *libovolný uživatel* — pro všechny uživatele (bez ohledu na to, zda jsou na firewallu ověřeni či nikoliv)
- *libovolný uživatel ověřený na firewallu* — pro všechny uživatele, kteří jsou přihlášeni
- *vybraní uživatelé* — pro vybrané uživatele a/nebo skupiny uživatelů.

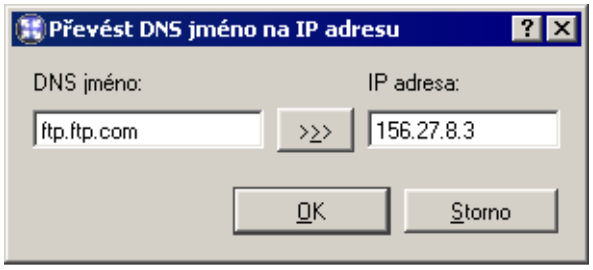
Tlačítko *Nastavit* otevírá dialog pro výběr uživatelů a skupin (přidržením kláves *Ctrl* a *Shift* můžete vybrat více uživatelů / skupin současně).

Poznámka: Povolení nebo omezení vztahující se na vybrané uživatele (případně na všechny přihlášené uživatele) má smysl pouze v kombinaci s pravidlem zakazujícím přístup nepřihlášeným uživatelům.

A FTP server vyhovuje těmto kritériím Specifikace FTP serverů, pro které má toto pravidlo platit:

- *libovolná IP adresa* — libovolný FTP server
- *IP adresa* — adresa konkrétního FTP serveru.

  Tlačítko *Převést* otevírá speciální dialog pro zjištění IP adresy z DNS jména (správce *WinRoute* není nucen otevřít příkazový řádek a použít např. příkaz `nslookup`).



  Do pole *DNS jméno* zadejte DNS jméno FTP serveru. Po stisknutí tlačítka *>>>* se v poli *IP adresa* objeví odpovídající IP adresa (získaná z DNS). Tlačítko *OK* zavře tento dialog a získaná IP adresa se automaticky vloží do pole *IP adresa* dialogu *Pravidlo pro FTP*.

- *IP adresa ze skupiny* — výběr skupiny IP adres FTP serverů, které mají být zakázány nebo povoleny.

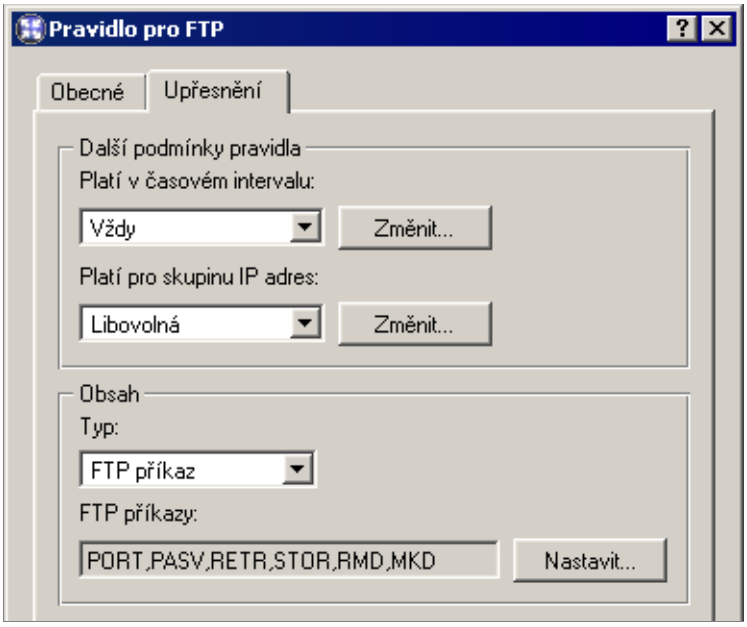
  Tlačítko *Změnit* otevírá dialog pro úpravu skupin IP adres (podrobnosti viz kapitola 8.1).

Akce Volba akce, která bude provedena, jestliže jsou splněny podmínky pro uživatele a FTP server:

- *Povolit přístup na FTP server*
- *Zakázat přístup na FTP server* — *WinRoute* bude blokovat určité FTP příkazy či celé spojení (v závislosti na nastavení v záložce *Upřesnění* — viz dále).

Zaškrtnutím volby *Zaznamenat* budou všechny přístupy na FTP, které vyhověly tomuto pravidlu, zaznamenány do záznamu *Filter* (viz kapitola 12.4).

V záložce *Upřesnění* jsou obsaženy další podmínky, za kterých má pravidlo platit, a volby pro FTP komunikaci.



Platí v časovém intervalu Výběr časového intervalu platnosti pravidla (mimo tento interval je pravidlo neaktivní). Tlačítko *Změnit* otevírá dialog pro úpravu časových intervalů (podrobnosti viz kapitola 8.2).

Platí pro skupinu IP adres Výběr skupiny IP adres, pro kterou bude toto pravidlo platit (jedná se o zdrojové IP adresy, tedy adresy klientů). Speciální volba *Libovolná* znamená, že pravidlo nebude závislé na IP adrese klienta.

Tlačítko *Změnit* otevírá dialog pro úpravu skupin IP adres (podrobnosti viz kapitola 8.1).

Obsah Upřesňující volby pro obsah FTP komunikace.

Volba *Typ* nastavuje způsob filtrování:

- *Download*, *Upload*, *Download / Upload* přenos souborů v některém směru, případně v obou směrech.

  Při výběru některé z těchto voleb se zobrazí položka *Jméno souboru* — v této položce můžete uvést jména souborů, pro které má pravidlo platit. Ve jméně souboru lze použít hvězdičkovou konvenci (např. `*.exe` — spustitelné soubory).

- *FTP příkaz* — výběr příkazů protokolu FTP, pro které má pravidlo platit

- *Libovolná* — zakazuje jakékoli připojení nebo příkaz, jakoukoli komunikaci

Nové pravidlo bude přidáno pod pravidlo, které bylo označené před stisknutím tlačítka *Přidat*. Šipkovými tlačítky na pravé straně okna přesuňte vytvořené pravidlo na požadované místo.

Zaškrtávací pole vedle popisu pravidla slouží k jeho „vypnutí“ — pravidlo můžete dočasně vyřadit bez nutnosti jej odstraňovat a poté znovu přidávat.

Poznámka: Přístup k FTP serverům, pro které neexistuje odpovídající pravidlo, je povolen (implicitně vše povoleno). Chceme-li povolit přístup pouze k omezené skupině FTP serverů a všechny ostatní stránky blokovat, je třeba na konec seznamu umístit pravidlo zakazující přístup ke všem FTP serverům.

6.6 Antivirová kontrola HTTP a FTP

WinRoute umožňuje kontrolovat objekty (soubory) přenášené protokoly HTTP a FTP antivirovým programem. Správce může specifikovat, které objekty (resp. typy objektů) mají být kontrolovány.

Přenášená data jednotlivých objektů jsou postupně ukládána do vyrovnávací paměti a kontrolována antivirem. Je-li nalezen virus, pak *WinRoute* nepošle klientovi poslední část souboru, kterou má dosud ve vyrovnávací paměti (zahodí ji). Klient tak dostane soubor poškozený — nebude jej moci spustit a virus aktivovat.

Upozornění: Antivirová kontrola dokáže pouze nalézt a blokovat infikované soubory, není možné je léčit!

Licence antivirového programu musí splňovat licenční podmínky dané jeho výrobcem (typicky stejný nebo vyšší počet uživatelů, pro který je licencován *WinRoute*, nebo speciální serverová licence).

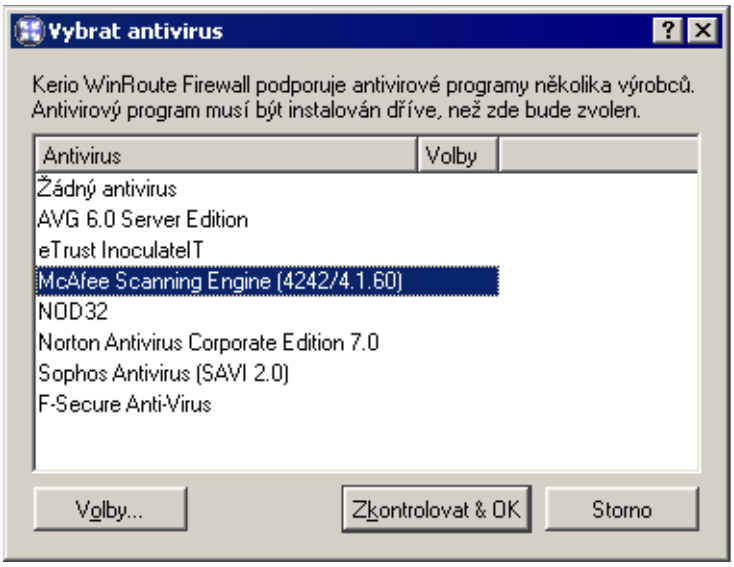
WinRoute je rovněž dodáván ve speciální verzi s integrovaným antivirem *McAfee*. Externí *McAfee Anti-Virus* není ve *WinRoute* podporován.

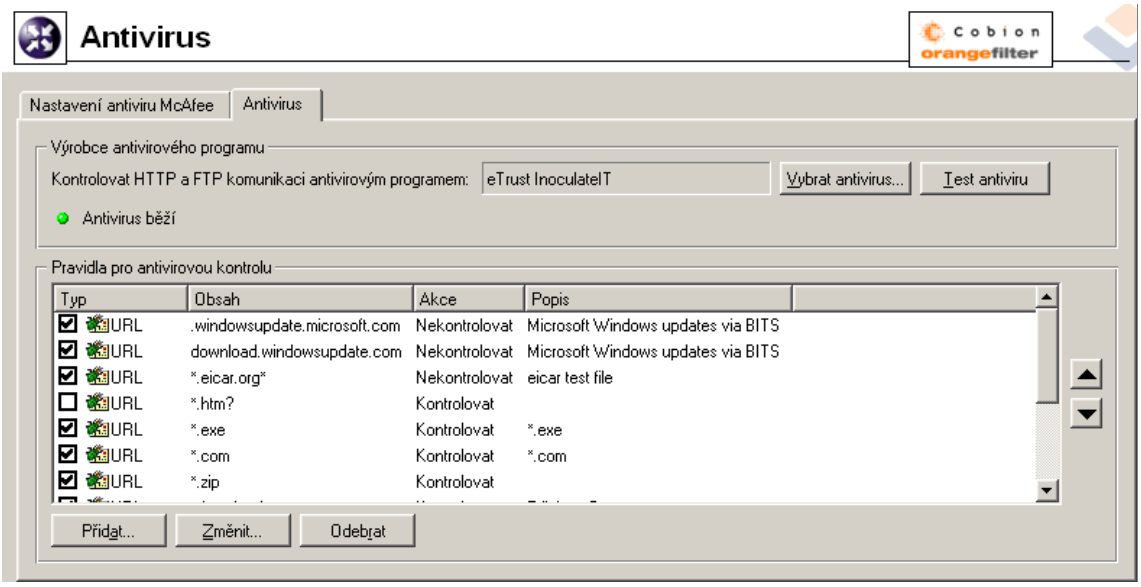
Parametry antivirové kontroly se nastavují v sekci *Konfigurace / Filtrování obsahu / Antivirus*.

Kontrolovat HTTP a FTP komunikaci antivirovým programem Toto pole zobrazuje antivirový program, který je používán pro kontrolu objektů přenášených protokoly HTTP a FTP. Výraz *(žádný)* znamená, že není nastaven žádný antivirus (antivirová kontrola nebude prováděna).

Vybrat antivirus... Toto tlačítko otevírá dialog pro výběr modulu pro spolupráci s antivirovým programem.

Antivirový program musí být nainstalován dříve, než jej zde vyberete (před instalací antivirového programu doporučujeme zastavit *WinRoute Firewall Engine*). Toto neplatí pro integrovaný antivirus *McAfee*, který je součástí *WinRoute*.





Po označení požadovaného antivirového modulu můžete tlačítkem *Volby* nastavit upřesňující parametry (jsou dostupné pouze u některých modulů). Tlačítko *Zkontrolovat & OK* provede test vybraného antiviru, a je-li test úspěšný, bude tento antivirus nadále používán. Je-li test neúspěšný, zůstane nastaven přechozí modul a do záznamu *Error* (viz kapitola 12.4) se zapíší příslušná chybová hlášení.

Volba *Žádný antivirus* vypíná antivirovou kontrolu.

Test antiviru Tlačítko umožňuje vyzkoušet antivirus pomocí testovacího viru (soubor Eicar). Pokud je virus nalezen, antivirus funguje.

Pravidla pro antivirovou kontrolu Tato pravidla slouží k nastavení podmínek, za kterých má být antivirová kontrola prováděna (implicitně se kontrolují všechny objekty přenášené protokoly HTTP a FTP).

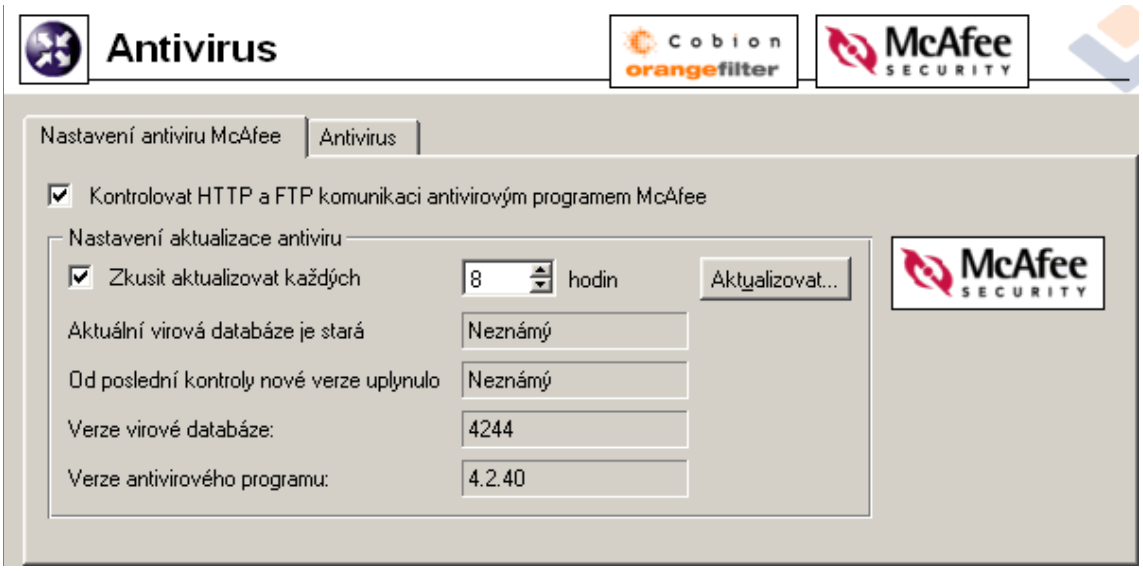
Poznámka: Instalace *WinRoute* obsahuje několik předdefinovaných pravidel pro antivirovou kontrolu. Ve výchozím nastavení se kontrolují všechny spustitelné soubory a soubory aplikací sady *Microsoft Office*. Správce *WinRoute* může toto nastavení upravit dle vlastního uvážení.

Podporované antivirové programy

WinRoute podporuje několik externích antivirových programů různých výrobců (např. Eset Software, Grisoft, F-Secure atd.). Podporované antiviry, stejně jako verze jednotlivých programů a obchodní podmínky, se však mohou měnit. Aktuální informace vždy naleznete na WWW stránkách firmy *Kerio Technologies* (`http://www.kerio.cz/`).

Integrovaný antivirus McAfee

Záložka *Nastavení antiviru McAfee* slouží k nastavení upřesňujících parametrů integrovaného antivirového programu *McAfee*.



Kontrolovat HTTP a FTP komunikaci ... Tlačítko zapne antivirovou kontrolu antivirovým programem *McAfee*.

Zkusit aktualizovat každých ... hodin Interval kontroly nových verzí virové databáze a antivirového programu (v hodinách). V těchto intervalech *WinRoute* zkontroluje, zda je k dispozici nějaká aktualizace, a pokud ano, automaticky ji stáhne.

Je-li pokus o aktualizaci neúspěšný (např. z důvodu nedostupnosti serveru), zapíše se detailní informace do záznamu *Error* (viz kapitola 12.4).

Při každém pokusu o aktualizaci se vynuluje položka *Od poslední kontroly nové verze uplynulo*.

Aktuální virová databáze je stará Stáří virové databáze, která je aktuálně používána.

Poznámka: Vysoká hodnota v tomto poli může indikovat, že se opakovaně nezdařilo databázi aktualizovat. V takových případech doporučujeme zkusit provést aktualizaci ručně (tlačítkem *Aktualizovat*) a prohlédnout záznam *Error*.

Od poslední kontroly nové verze uplynulo Doba, která uplynula od posledního pokusu o aktualizaci (bez ohledu na to, zda byl úspěšný či nikoliv).

Verze virové databáze Číslo verze virové databáze, která se aktuálně používá.

Verze antivirového programu Číslo verze antivirového modulu *McAfee*, který *WinRoute* používá.

Aktualizovat Toto tlačítko slouží k okamžitému provedení aktualizace (tj. kontroly a případného stažení nových verzí) virové databáze a antivirového programu.

Po stisknutí tlačítka *Aktualizovat* se zobrazí okno s průběhem aktualizace. Toto okno můžete tlačítkem *OK* kdykoliv zavřít — není třeba čekat na dokončení aktualizace.

Proběhne-li aktualizace úspěšně, zobrazí se číslo nové verze virové databáze a/nebo antivirového programu a stáří aktuální virové databáze. Je-li pokus o aktualizaci neúspěšný (např. z důvodu nedostupnosti serveru), zobrazí se chybové hlášení a zapíše se detailní informace do záznamu *Error*.

Při každém pokusu o aktualizaci se vynuluje položka *Od poslední kontroly nové verze uplynulo*.

Nastavení pravidel pro antivirovou kontrolu

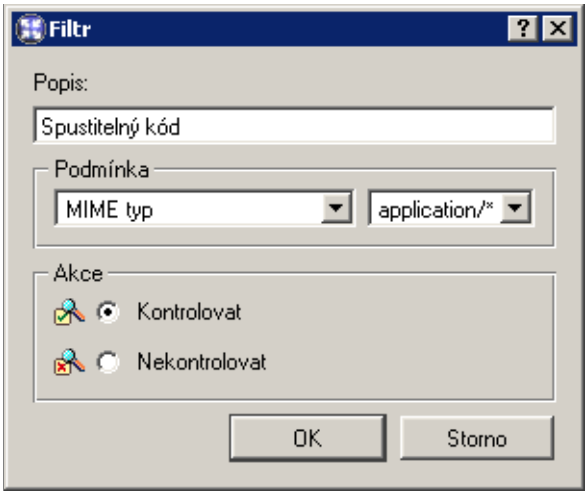
Pravidla antivirové kontroly tvoří uspořádaný seznam, který je procházen shora dolů. Tlačítky se šipkami na pravé straně okna lze upravit pořadí pravidel. Vyhodnocování se zastaví na prvním pravidle, kterému kontrolovaný objekt vyhoví.

Tlačítko *Přidat* otevírá dialog pro definici nového pravidla.

Popis Textový popis pravidla (pro snazší orientaci správce *WinRoute*)

Jestliže Podmínka pravidla:

- *MIME typ* objektu.



MIME typ může být zadán kompletně (např. `image/jpeg`) nebo s použitím hvězdičkové konvence (např. `application/*`).

- *URL* objektu (např. `www.kerio.com/img/logo.gif`), podřetězec s použitím hvězdičkové konvence (např. `*.exe`) nebo jméno serveru (např. `www.kerio.com`). Jméno serveru má význam libovolného URL na tomto serveru (`www.kerio.com/*`).

- *HTTP/FTP jméno souboru*

  Volbou lze filtrovat jména souborů (nikoli celá URL) přenášených protokolem FTP nebo HTTP (např. `*.exe`, `*.zip` ...).

Zadáme-li jako MIME typ nebo URL pouze hvězdičku, bude pravidlo platit pro všechny objekty.

pak Volba, zda objekt má či nemá být kontrolován antivirovým programem.

Nové pravidlo bude přidáno pod pravidlo, které bylo označené před stisknutím tlačítka *Přidat*. Šipkovými tlačítky na pravé straně okna přesuňte vytvořené pravidlo na požadované místo.

Zaškrtávací pole vedle popisu pravidla slouží k jeho „vypnutí“ — pravidlo můžete dočasně vyřadit bez nutnosti jej odstraňovat a poté znovu přidávat.

Poznámka: Nevyhoví-li objekt žádnému pravidlu, pak je antivirovým programem automaticky zkontrolován. Chcete-li kontrolovat pouze vybrané typy objektů, uveďte na konec seznamu pravidlo zakazující antivirovou kontrolu pro libovolné URL či libovolný MIME typ.

Kapitola 7

WWW rozhraní a ověřování uživatelů

WinRoute obsahuje speciální WWW server, který poskytuje rozhraní pro přihlašování uživatelů, ovládání vytáčených linek a správu cache. WWW rozhraní existuje ve dvou verzích: nezabezpečené a zabezpečené SSL (obě verze obsahují totožné stránky).

V následujícím přehledu uvádíme seznam URL jednotlivých stránek (`server` má význam jména nebo IP adresy počítače s *WinRoute* a `4080` je standardní port WWW rozhraní).

- hlavní stránka (*Index*) — obsahuje pouze odkazy na dále uvedené stránky

  `http://server:4080/`

- ověřování uživatelů na firewallu (přihlašovací a odhlašovací stránka)

  `http://server:4080/fw/login`

  `http://server:4080/fw/logout`

- zobrazení statistik uživatele (IP adresa, doba přihlášení, objem přenesených dat, počet filtrovaných objektů...)

  `http://server:4080/fw/stat`

- změna uživatelských nastavení (heslo, globální omezení pro WWW)

  `http://server:4080/fw/pref`

- zobrazení pravidel pro HTTP (viz kapitola 6.1), která se vztahují na daného uživatele a počítač, z něhož se k WWW rozhraní připojuje

  `http://server:4080/fw/http_restr`

- zobrazení statistik HTTP cache s možností vyhledávání a mazání uložených objektů

  `http://server:4080/fw/cache`

- vytáčení a zavěšování vytáčených linek

  `http://server:4080/fw/dial`

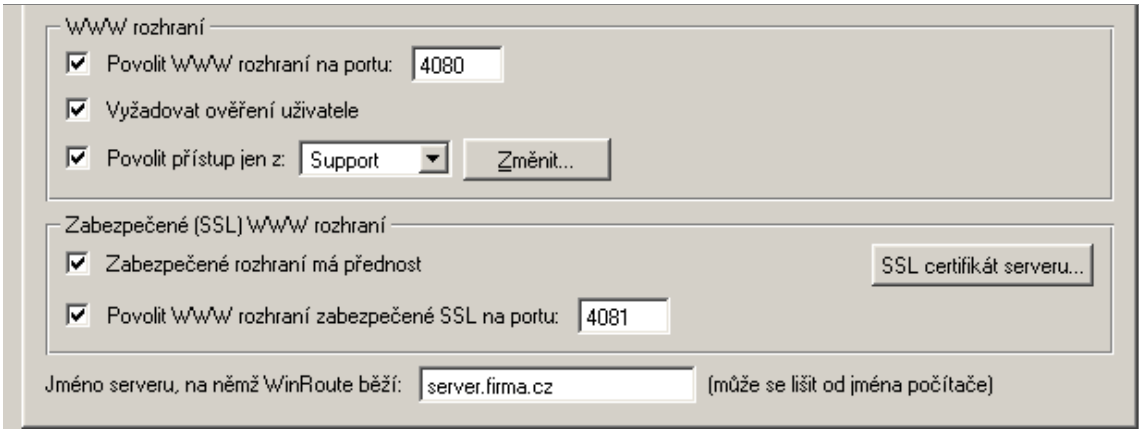
Pro zabezpečenou verzi je třeba uvést protokol HTTPS a port, na němž zabezpečené WWW rozhraní běží (standardně `4081`) — např.:

```
https://server:4081/fw/login
```

Poznámka: V následujících kapitolách budou pro jednoduchost jako příklady uváděna pouze URL stránek nezabezpečeného WWW rozhraní. Vždy platí, že zadáním protokolu HTTPS a příslušného čísla portu lze přistoupit na zabezpečenou verzi téže stránky.

7.1 Nastavení parametrů WWW rozhraní

Základní parametry WWW rozhraní *WinRoute* lze nastavit v sekci *Konfigurace / Další volby*, záložka *Ověřování uživatele*.



Poznámka: Popis první sekce záložky *Ověřování uživatele* naleznete v kapitole 7.2.

Povolit WWW rozhraní na portu Číslo portu, na němž poběží nezabezpečená (HTTP) verze WWW rozhraní. Výchozí hodnota je 4080.

Vyžadovat ověření uživatele Po zapnutí této volby bude při přístupu na stránky vytáčení linek a zobrazení obsahu cache vyžadováno přihlášení uživatele. Při přístupu na tyto stránky z počítače, z něhož není přihlášen žádný uživatel, dojde k automatickému přesměrování prohlížeče na přihlašovací stránku.

Povolit přístup jen z Výběr skupiny IP adres, z níž bude k WWW rozhraní povolen přístup.

Správce *WinRoute* může povolit přístup k WWW rozhraní z určitých IP adres bez nutnosti přihlášení uživatele nebo kombinovat tuto volbu s volbou *Vyžadovat ověření uživatele* pro zvýšení bezpečnosti WWW rozhraní.

Poznámka: Výše uvedené volby *Vyžadovat ověření uživatele* a *Povolit přístup jen z* se vztahují k nezabezpečené i zabezpečené verzi WWW rozhraní.

Zabezpečené rozhraní má přednost Po aktivaci této volby bude uživatel vždy přesměrován na zabezpečenou verzi přihlašovací stránky nebo stránky informující o zakázaném přístupu. Tímto se zabrání odposlechu jména a hesla uživatele (viz dále).

Povolit WWW rozhraní zabezpečné SSL na portu Číslo portu, na němž poběží zabezpečená (HTTPS) verze WWW rozhraní. Výchozí hodnota je `4081`.

Jméno serveru... DNS jméno serveru, které bude použito pro účely WWW rozhraní (např. `server.firma.cz`). Toto jméno nemusí být vždy totožné s názvem počítače, ale musí pro něj existovat odpovídající záznam v DNS.

Poznámka: Pokud všichni klienti, kteří na WWW rozhraní přistupují, používají jako DNS server *DNS Forwarder* ve *WinRoute*, pak není nutné jméno serveru do DNS přidávat — *DNS Forwarder* jej přečte automaticky z této položky (a provede rovněž kombinaci se jménem lokální domény — viz kapitola 4.2).

SSL certifikát serveru Toto tlačítko otevírá dialog pro import nebo vytvoření certifikátu serveru pro komunikaci protokolem SSL (tj. pro zabezpečenou verzi WWW rozhraní). Podrobnosti viz dále.

Upozornění: Zadáme-li do položky *Povolit WWW rozhraní na portu* nebo *Povolit WWW rozhraní zabezpečené SSL na portu* port, který již používá jiná služba či aplikace, pak po stisknutí tlačítka *Použít WinRoute* tento port sice akceptuje, ale WWW rozhraní se na něm nespustí a do záznamu *Error* (viz kapitola 12.4) se vypíše chybové hlášení v této podobě:

```
failed to bind to port 4080: another application is using this
port
```

Pokud nemáte jistotu, že zadané porty jsou skutečně volné, pak bezprostředně po stisknutí tlačítka *Použít* zkontrolujte záznam *Error*, zda se v něm takovéto hlášení neobjevilo.

Jazyk WWW rozhraní

WWW rozhraní *WinRoute* je k dispozici ve více jazykových verzích. Jazyk se volí automaticky dle nastavených preferencí ve WWW prohlížeči klienta (tato možnost existuje téměř ve všech současných prohlížečích). Není-li k dispozici žádný z preferovaných jazyků, použije se výchozí — angličtina.

Jednotlivé jazykové verze jsou uloženy v tzv. definičních souborech v podadresáři `weblang` adresáře, kde je *WinRoute* nainstalován. Každý jazyk tvoří dva soubory: `xx.def` a `xx.res`, kde `xx` představuje standardní dvoupísmennou zkratku jazyka (např. `en` pro angličtinu, `cs` pro češtinu apod.). Na prvním řádku souboru `xx.def` je uvedena zkratka jazyka (shodná se zkratkou v názvu souboru) a na druhém řádku kódování znaků pro

daný jazyk (např. `ISO-8859-2` pro češtinu). Toto kódování znaků musejí používat oba soubory pro daný jazyk.

Z výše uvedeného popisu vyplývá, že správce *WinRoute* může poměrně snadno modifikovat texty jednotlivých stránek WWW rozhraní, případně vytvořit novou jazykovou verzi.

Poznámka: Změny v souboru `xx.def` se projeví až po restartu *WinRoute Firewall Engine*.

SSL certifikát serveru

Princip zabezpečeného WWW rozhraní *WinRoute* spočívá v tom, že se celé spojení mezi klientem a serverem šifruje, aby bylo zabráněno odposlechu a zneužití přenášených informací. Protokol SSL, který je k tomuto účelu využit, používá nejprve asymetrickou šifru pro výměnu symetrického šifrovacího klíče, kterým se pak šifrují vlastní přenášená data.

Asymetrická šifra používá dva klíče: veřejný pro šifrování a privátní pro dešifrování. Jak už jejich názvy napovídají, veřejný (šifrovací) klíč má k dispozici kdokoliv, kdo chce navázat se serverem spojení, zatímco privátní (dešifrovací) klíč má k dispozici pouze server a musí zůstat utajen. Klient ale také potřebuje mít možnost, jak si ověřit identitu serveru (zda je to skutečně on, zda se za něj pouze někdo nevydává). K tomu slouží tzv. certifikát. Certifikát v sobě obsahuje veřejný klíč serveru, jméno serveru, dobu platnosti a některé další údaje. Aby byla zaručena pravost certifikátu, musí být ověřen a podepsán třetí stranou, tzv. certifikační autoritou.

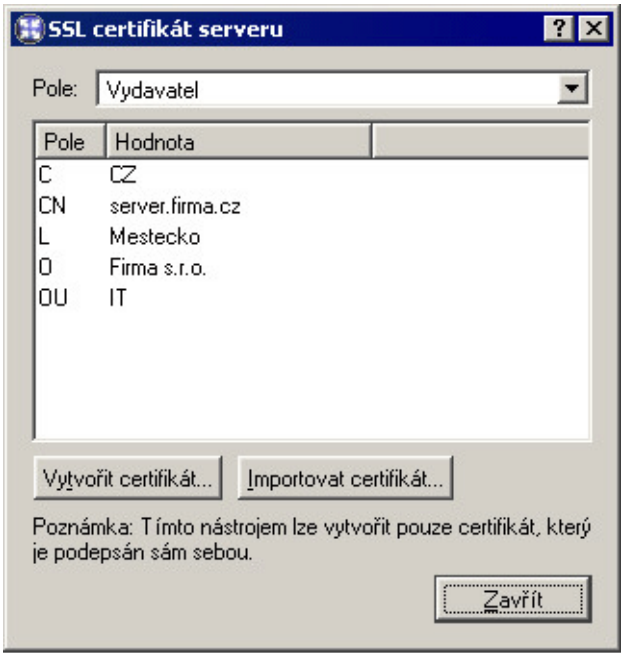
Komunikace mezi klientem a serverem pak vypadá následovně: Klient vygeneruje symetrický klíč a zašifruje ho veřejným klíčem serveru (ten získá z certifikátu serveru). Server jej svým privátním klíčem (který má jen on) dešifruje. Tak znají symetrický klíč jen oni dva a nikdo jiný.

Import nebo vytvoření SSL certifikátu

WinRoute je standardně dodáván s testovacím certifikátem, který byl vytvořen pro zkušební účely. Je uložen v podadresáři `sslcert` adresáře, kde je *WinRoute* nainstalován, v souboru `server.crt`. Soubor `server.key` obsahuje privátní klíč serveru. Tento certifikát je ale ve všech distribucích *WinRoute* stejný, a proto zajišťuje pouze funkčnost zabezpečených služeb, ale prakticky žádnou bezpečnost (privátní klíč je veřejně známý — kdokoliv tedy může dešifrovat komunikaci zabezpečenou příslušným veřejným klíčem).

Po stisknutí tlačítka *SSL certifikát serveru* (sekce *Konfigurace / Další volby* záložka *Ověřování uživatele*) se zobrazí dialog s aktuálním certifikátem serveru. Volbou *Pole* (položka

certifikátu) lze zobrazit údaje buď o vydavateli certifikátu (*Vydavatel*) nebo o subjektu (*Předmět*) — tedy vašem serveru.



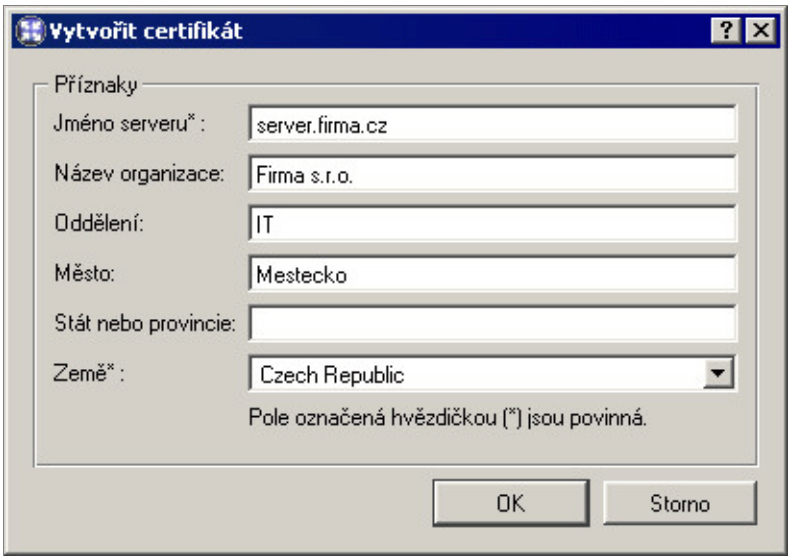
Vlastní originální certifikát, který bude skutečně prokazovat identitu vašeho serveru, můžete získat dvěma způsoby.

Můžete si vytvořit vlastní, tzv. self-signed certifikát (tj. podepsaný sám sebou). To lze provést stisknutím tlačítka *Vytvořit certifikát* v dialogu, kde se zobrazuje aktuální certifikát serveru. V dialogu, který se zobrazí, je třeba vyplnit údaje o serveru a vaší společnosti. Povinné jsou pouze položky označené hvězdičkou (*).

Po stisknutí tlačítka *OK* se nově vytvořený certifikát zobrazí v dialogu *SSL certifikát serveru* a ihned začne používat (není třeba nic restartovat).

Vytvořený certifikát je originální a je vystaven vaší firmou vaší firmě na jméno vašeho serveru (self-signed certifikát — certifikujete sami sebe). Narozdíl od testovacího certifikátu, tento již zajišťuje vašim klientům bezpečnost, protože příslušný privátní klíč znáte pouze vy a certifikát prokazuje identitu vašeho serveru. Klienti budou ve svých prohlížečích upozorněni již pouze na to, že certifikát nevystavila důvěryhodná certifikační autorita. Protože však vědí, kdo tento certifikát vytvořil a proč, mohou si jej do prohlížeče nainstalovat. Tím mají zajištěnu bezpečnou komunikaci a žádné varování se jim již zobrazovat nebude, protože váš certifikát nyní splňuje všechny potřebné náležitosti.

Druhou možností je získat plnohodnotný certifikát od některé veřejné certifikační autority (např. Verisign, Thawte, SecureSign, SecureNet, Microsoft Authenticode apod.). Prů-



běh certifikace je poměrně složitý a vyžaduje určité odborné znalosti. Jeho popis je nad rámec tohoto manuálu.

7.2 Ověřování uživatelů na firewallu

WinRoute umožňuje kontrolu přístupu (filtrování paketů/spojení, WWW stránek a FTP objektů a příkazů) na základě uživatele. Jméno uživatele ve filtrovacím pravidle má význam IP adresy počítače, z něhož je tento uživatel přihlášen (resp. všech počítačů, z nichž je v daném okamžiku přihlášen).

Kromě omezování přístupu lze přihlašování uživatelů využít také pro sledování jejich aktivit v záznamech (viz kapitola12.4), přehledu otevřených spojení (viz kapitola12.3) a přehledu počítačů a uživatelů (viz kapitola12.2). Není-li z určitého počítače přihlášen žádný uživatel, objeví se v záznamech a přehledech pouze IP adresa tohoto počítače.

Uživatel se může k firewallu přihlásit těmito způsoby:

- ručně — ve svém prohlížeči otevře stránku

  ```
  http://server:4080/fw/login
  ```

- přesměrováním — přístupem na WWW stránku, na kterou je povolen přístup pouze přihlášenému uživateli

- prostřednictvím NTLM — je-li použit prohlížeč *Microsoft Internet Explorer* a uživatel se ověřuje ve Windows NT nebo Windows 2000 doméně, pak může být ověřen zcela automaticky (přihlašovací stránka se vůbec nezobrazí). Podrobnosti viz dále (odstavec *Volby pro ověřování uživatelů*).

Přihlášení přesměrováním probíhá následovně: uživatel zadá do prohlížeče adresu stránky, kterou chce navštívit. *WinRoute* zjistí, že uživatel dosud není přihlášen, a automaticky jej přesměruje na přihlašovací stránku. Po úspěšném přihlášení je uživatel ihned přesměrován na požadovanou stránku nebo se zobrazí stránka s informací, že na tuto stránku má přístup zakázán.

Poznámka: Pokud je v parametrech WWW rozhraní zapnuta volba *Zabezpečené WWW rozhraní má přednost* (viz kapitola 7.1), pak jsou uživatelé automaticky přesměrováváni na zabezpečenou přihlašovací stránku, v opačném případě na nezabezpečenou.

Přihlašovací stránka

Dialog pro přihlášení na přihlašovací stránce má následující podobu:

Uživatelské jméno, Heslo Přihlašovací jméno a heslo uživatele.

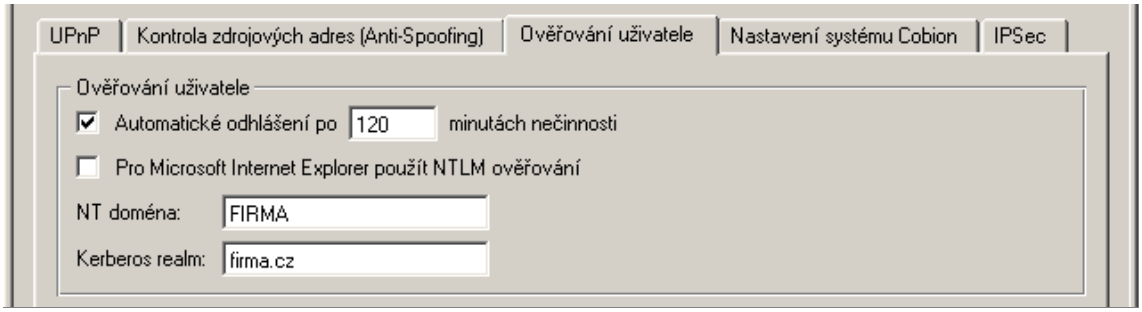
Zobrazit stránku uživatelských nastavení Po úspěšném přihlášení dojde k automatickému přesměrování na uvítací stránku, z níž lze přejít na stránku uživatelských nastavení, statistik nebo původně požadovanou stránku (detaily viz kapitola 7.3).

Pokud byl uživatel na přihlašovací stránku přesměrován automaticky (zadáním URL stránky, pro niž firewall vyžaduje ověření), bude po úspěšném přihlášení přesměrován na původní požadovanou stránku. Toto neplatí při zaškrtnutí volby *Zobrazit stránku uživatelských nastavení*, kde se zobrazí uvítací stránka (na ní je umístěn odkaz na původně požadovanou stránku). Podrobnosti najdete v kapitole 7.3.

Volby pro ověřování uživatelů

Volitelné parametry pro ověřování uživatelů lze nastavit v sekci *Konfigurace / Další volby*, záložka *Ověřování uživatele*, oddíl *Ověřování uživatele*.

Automatické odhlášení po ... Doba (v minutách), po níž dojde k automatickému odhlášení uživatele od firewallu, jestliže z jeho počítače není zaznamenána žádná komunikace. Výchozí hodnota je 120 minut (2 hodiny).



Tato situace nastává zpravidla v případech, kdy se uživatel zapomene od firewallu odhlásit, a proto nedoporučujeme tuto volbu vypínat (nastavením hodnoty 0) — mohlo by totiž dojít k tomu, že získaná přístupová práva budou zneužita jiným uživatelem (přičemž bude ve všech záznamech figurovat jméno uživatele, který se zapomněl odhlásit).

Pro Microsoft Internet Explorer... Jestliže je použit prohlížeč *Microsoft Internet Explorer* (verze 5.01 a vyšší), pak může být uživatel ověřován na firewallu automaticky (pomocí NTLM autentizace). Tento způsob ověřování funguje správně pouze za dodržení následujících podmínek:

1. Server (tj. počítač s *WinRoute*) musí být členem příslušné Windows NT nebo Windows 2000 domény.
2. Klientský počítač musí být rovněž členem této domény.
3. Uživatel na klientském počítači se musí přihlašovat do této domény (tzn. není možno použít lokální uživatelský účet).
4. *WinRoute Firewall Engine* musí běžet jako služba nebo musí být spouštěn pod uživatelem, který má administrátorská práva k počítači.
5. NTLM autentizaci není možné použít pro ověřování v interní databázi.

Ověřovat uživatele v NT doméně Jméno NT domény, v níž mají být uživatelé ověřováni (např. `FIRMA`). V této položce může být uvedeno více domén oddělených středníkem.

Kerberos realm Název oblasti (domény) systému Kerberos, ve které mají být uživatele ověřováni (např. `firma.cz`). Můžete uvést více domén oddělených středníkem.

Tento způsob ověřování používá doména Windows 2000 (*Active Directory*).

Poznámka: Při importu uživatelských účtů z NT domény nebo Windows 2000 domény se příslušná položka vyplní automaticky.

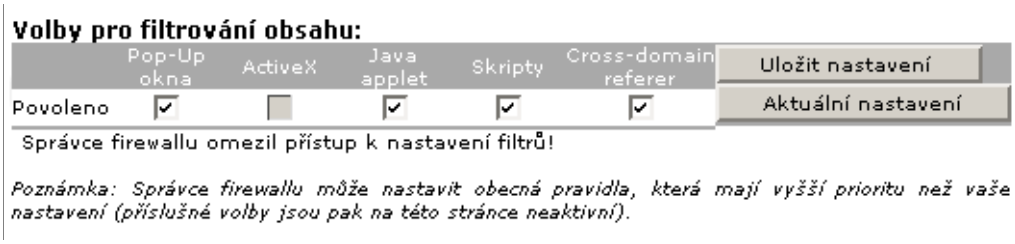
7.3 Uživatelské preference a statistiky

Pokud uživatel požadoval zobrazení stránky uživatelských nastavení (zaškrtnutím stejnojmenné volby na přihlašovací stránce), pak je po úspěšném přihlášení uživatel automaticky přesměrován na tzv. uvítací stránku. Tato stránka obsahuje (mimo jiné) odkazy na:

- původně požadovanou stránku (*URL:*) — pokud nebyla přihlašovací stránka vyvolána automaticky, je tato položka prázdná
- stránku preferencí uživatele (*Uživatelská nastavení*)
- stránku statistik uživatele (*Statistiky*)

Uživatelská nastavení

První část stránky uživatelských preferencí umožňuje povolit či zakázat určité prvky v HTML stránkách.



Volby pro filtrování obsahu Zaškrtnutí políčka pod názvem prvku znamená, že tento prvek bude povolen (tzn. nebude firewallem blokován). Je-li ve *WinRoute* nastaveno globální omezení určitého prvku (viz kapitola 6.2) a uživatel nemá právo *přejít pravidla pro obsah WWW stránek* (viz kapitola 9.1), pak je příslušné pole na této stránce neaktivní (uživatel nemůže nastavení měnit). V tomto případě smí uživatel své nastavení pouze zpřísnit — nemůže povolit HTML prvek, který je globálně zakázán.

- *Pop-Up okna* — automatické otevírání nových oken prohlížeče — typicky reklamy.

  Tato volba blokuje ve skriptech metodu `window.open()`.

- *ActiveX* — prvky Microsoft ActiveX (tato technologie dovoluje mimo jiné např. spouštění aplikací na klientském počítači).

  Tato volba blokuje HTML tagy `<object>` a `<embed>`.

- *Java applet* — blokování HTML tagů `<applet>`

- *Skripty* — blokování HTML tagů `<script>` (příkazy jazyků JavaScript, VBScript atd.)

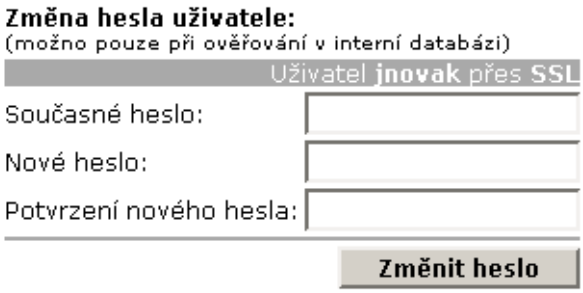
- *Cross-domain referer* — blokování položek `Referer` v HTTP hlavičce. Tato položka obsahuje URL stránky, z níž klient na danou stránku přešel. Volba *Cross-domain referer* blokuje položku `Referer` v případě, že obsahuje jiné jméno serveru než aktuální požadavek.

  Blokování *Cross-domain referer* má význam pro ochranu soukromí uživatele (položka `Referer` může být sledována pro zjištění, jaké stránky uživatel navštěvuje).

Uložit nastavení Stisknutím tohoto tlačítka se nastavené volby uloží a aktivují.

Aktuální nastavení Toto tlačítko obnoví nastavení, které je momentálně aktivní (tj. jako při otevření této stránky, resp. při posledním stisknutí tlačítka *Uložit nastavení*).

Druhá část stránky slouží pro změnu hesla uživatele.



Do příslušných položek je třeba zadat aktuální heslo uživatele, nové heslo a zopakovat nové heslo pro potvrzení. Tlačítkem *Změnit heslo* se nové heslo uloží.

Upozornění: Změna hesla je možná pouze v případě, kdy je uživatel ověřován v interní databázi *WinRoute* (viz kapitola 9.1). Je-li použita jiná metoda ověřování, *WinRoute Firewall Engine* nemůže heslo uživatele změnit.

Statistiky

Na stránce *Statistiky uživatele* jsou zobrazovány tyto údaje:

- *Informace o přihlášení* — uživatelské jméno, IP adresa, z níž je uživatel přihlášen, doba přihlášení a metoda, kterou se přihlásil (*SSL* — zabezpečená přihlašovací strán-

ka, *Plaintext* — nezabezpečená přihlašovací stránka, *NTLM* — bezpečné ověření ve Windows NT nebo Windows 2000, *Proxy* — ověření na proxy serveru ve *WinRoute*)

- *Informace o relaci* — objem vyslaných a přijatých dat (v bytech) a počet vyslaných HTTP požadavků
- *Statistika filtrování obsahu* — počet odstraněných objektů jednotlivých typů (viz výše)

Všechny údaje jsou měřeny od posledního přihlášení uživatele. Při odhlášení uživatele (příp. zastavení *WinRoute Firewall Engine*) se statistiky nulují.

7.4 Zobrazení pravidel pro WWW stránky

Kliknutím na odkaz *Omezení WWW* na kterékoliv stránce WWW rozhraní *WinRoute* se zobrazí aktuální omezení přístupu na WWW stránky vztahující se na daný počítač a přihlášeného uživatele. Není-li přihlášen žádný uživatel, zobrazí se omezení platná pro IP adresu počítače, z něhož se k WWW rozhraní přistupuje.

Detailní informace o pravidlech pro WWW stránky naleznete v kapitole 6.1.

7.5 Ovládání vytáčených linek

Stránka *Vytáčené linky* zobrazuje seznam všech vytáčených linek, které jsou ve *WinRoute* definovány (viz kapitola 4.1). U každé linky je zobrazen:

- stav linky — připojeno (*Connected*) nebo zavěšeno (*Disconnected*)
- příkaz (v závislosti na stavu linky) —vytočit (*Dial*) nebo zavěsit (*Hang up*)

Poznámka: Stránka *Vytáčené linky* je v pravidelných intervalech automaticky obnovována, aby stále zobrazovala aktuální stav linek.

Tuto stránku (tj. stav vytáčených linek) si může zobrazit libovolný uživatel (není vyžadováno přihlášení). Po kliknutí na příkaz (*Dial* nebo *Hang up*) se však kontroluje, zda WWW rozhraní vyžaduje ověření uživatele (viz kapitola 7.1). Pokud ano, dojde k automatickému přesměrování na přihlašovací stránku. Uživatel, který chce ovládat vytáčené linky, musí mít odpovídající práva (volba *Uživatel má právo vytočit linku* v definici uživatelského účtu — viz kapitola 9.1).

7.6 Správa HTTP cache

Stránka *Obsah cache* WWW rozhraní *WinRoute* slouží pro zobrazení a mazání objektů v HTTP cache. Tuto stránku může otevřít (zadáním příslušného URL nebo odkazem

Cache v zápatí kterékoliv stránky WWW rozhraní) pouze uživatel, který má alespoň právo pro čtení konfigurace *WinRoute*. Pro mazání objektů z cache jsou třeba plná práva ke správě. Detailní informace o přístupových právech uživatelů najdete v kapitole 9.1.

Poznámka: Nastavení parametrů HTTP cache je popsáno v kapitole 4.5.

Kliknutím na odkaz *Více informací* se v přehledných tabulkách zobrazí:

- Počet uložených souborů, celková velikost všech souborů a průměrná velikost souboru
- Tabulka rozložení velikostí souborů (po 1 KB)
- Počet nalezených a nenalezených objektů v cache
- Informace o prováděných údržbách cache (počet, čas uplynulý od poslední údržby a doba jejího trvání)

Pole *URL:* s tlačítkem *Vypsat* slouží pro vyhledání všech objektů vyhovujících zadané masce URL. Nalezené objekty jsou vypsány v přehledné tabulce (max. 100 záznamů). U každého objektu je zobrazena jeho velikost, aktuální životnost (TTL) v hodinách a odkaz *Smazat* pro vymazání tohoto objektu z cache.

Kliknutím na odkaz *Smazat vše* lze vymazat z cache všechny objekty vyhovující zadané masce URL (nikoliv pouze prvních 100 objektů, které jsou zobrazeny v tabulce).

TIP: Volbou *Smazat vše* můžete vymazat celý obsah cache, jestliže do pole *URL:* zadáte pouze hvězdičku (*).

Kapitola 8

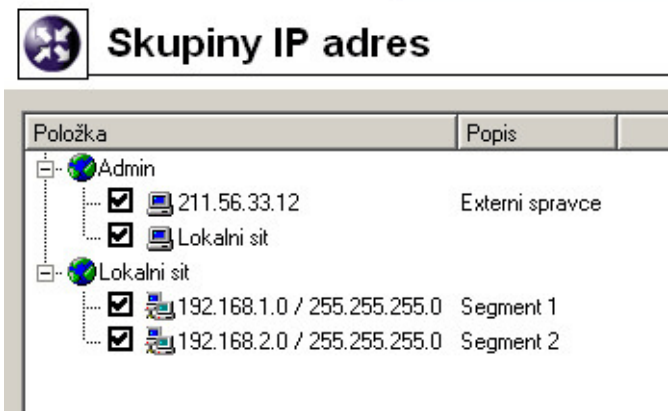
Definice

8.1 Skupiny IP adres

Skupiny IP adres slouží k jednoduchému nastavení přístupu k určitým službám (např. vzdálená správa *WinRoute*, WWW server v lokální síti zpřístupněný z Internetu atd.). Při nastavování přístupu se použije jméno skupiny, a ta pak může obsahovat libovolné kombinace jednotlivých počítačů (IP adres), rozsahů IP adres, subsítí či jiných skupin.

Vytvoření či úprava skupiny IP adres

Definice skupin IP adres se provádí v sekci *Konfigurace / Definice / Skupiny IP adres*.



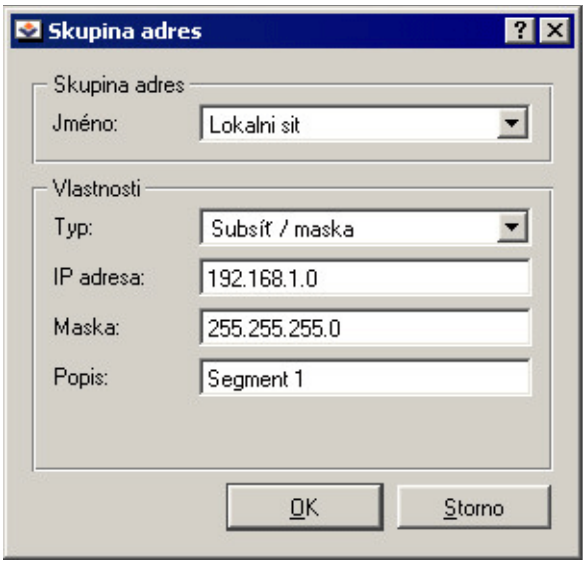
Tlačítkem *Přidat* lze přidat novou skupinu (nebo položku do existující skupiny), tlačítkem *Změnit* upravit a tlačítkem *Odebrat* smazat vybranou skupinu či položku.

Po stisknutí tlačítka *Přidat* se zobrazí dialog pro vytvoření nové skupiny IP adres.

Jméno Název skupiny. Zadáním nového (dosud neexistujícího) názvu se vytvoří nová skupina, zadáním názvu již existující skupiny se přidá nová položka do této skupiny.

Typ Druh přidávané položky. Možnosti: jedna IP adresa (*Počítač*), rozsah IP adres (*Subsíť / rozsah*), subsíť s příslušnou maskou (*Subsíť / maska*) nebo jiná skupina IP adres (*Skupina adres*). Skupiny adres lze do sebe vnořovat.

IP adresa, Maska... Parametry přidávané položky (v závislosti na zvoleném typu)



Popis Textový popis (komentář) ke skupině IP adres. Slouží pouze pro potřeby správce.

Poznámka: Každá skupina IP adres musí obsahovat alespoň jednu položku. Odebráním poslední položky skupina zanikne.

8.2 Časové intervaly

Časové intervaly jsou ve *WinRoute* úzce propojeny s komunikačními pravidly (viz kapitola 5). Správce *WinRoute* má tak možnost nastavit časový interval, kdy bude dané pravidlo platit. Ve skutečnosti se nejedná o interval, ale o skupinu tvořenou libovolným počtem různých intervalů a jednorázově naplánovaných akcí.

Druhým využitím časových intervalů je nastavení parametrů vytáčených linek — viz kapitola4.1.

Časové intervaly se definují v sekci *Konfigurace / Definice / Časové intervaly*.

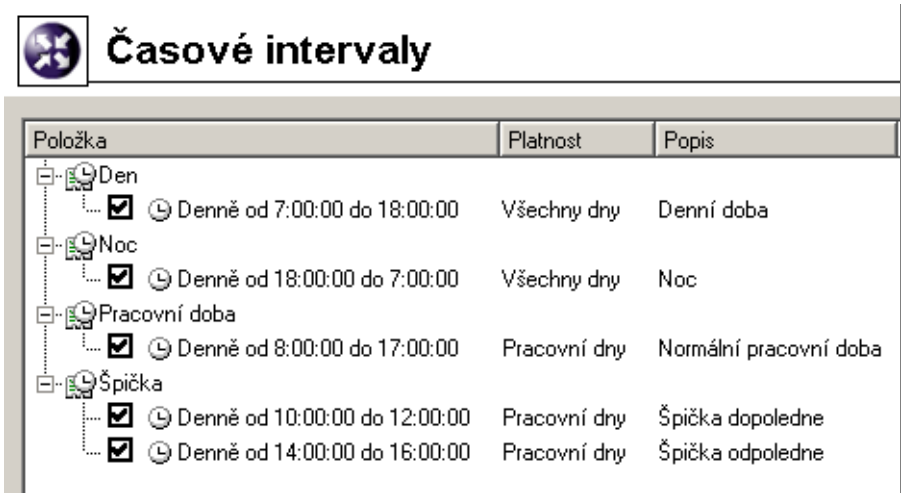
Platnost časového intervalu

Při definici časového intervalu lze použít tři druhy časových úseků (subintervalů):

Absolutní Interval je přesně ohraničen počátečním a koncovým datem, neopakuje se

Týdenní Opakuje se každý týden (ve stanovených dnech)

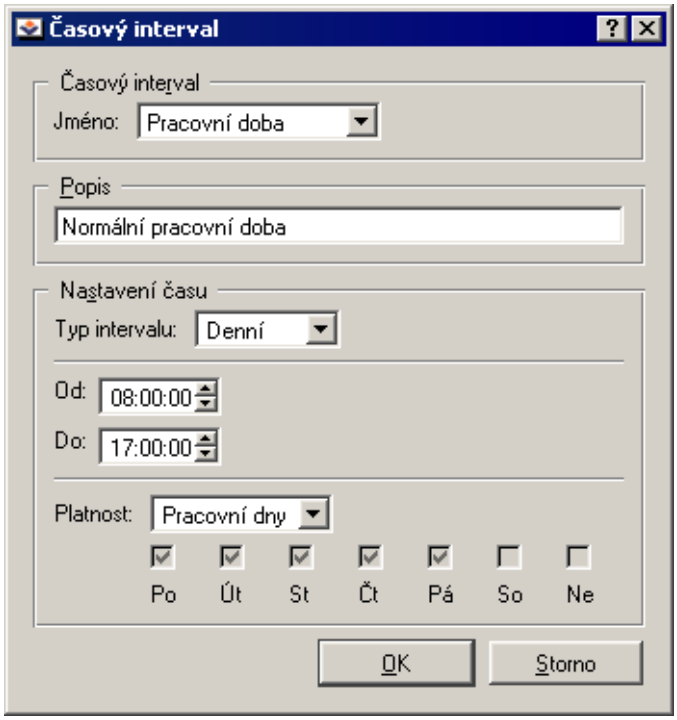
Denní Opakuje se každý den (ve stanovených hodinách)



Definice časových intervalů

Vytvoření, úpravu nebo smazání časového intervalu lze provést v sekci *Konfigurace / Definice / Časové intervaly*.

Po stisknutí tlačítka *Přidat* se zobrazí dialog pro definici časového intervalu:



Jméno Jednoznačný název (identifikace) časového intervalu. Zadáním nového (dosud neexistujícího) názvu se vytvoří nový časový interval, zadáním názvu již existujícího intervalu se přidá nová položka do tohoto intervalu.

Popis Textový popis intervalu (slouží pouze pro účely správce)

Typ intervalu Typ časového intervalu: *Denní*, *Týdenní* nebo *Absolutní* — začínající a končící konkrétním datem

Od, Do Začátek a konec časového úseku. Zde je možné zadat počáteční a koncový čas, případně také den v týdnu nebo datum (v závislosti na zvoleném typu intervalu)

Platnost Dny v týdnu, kdy je interval aktivní. Lze vybrat konkrétní dny (*Vybrané dny*), nebo použít některou přednastavenou volbu (*Všechny dny*, *Pracovní dny* — pondělí až pátek, *Víkend* — sobota a neděle).

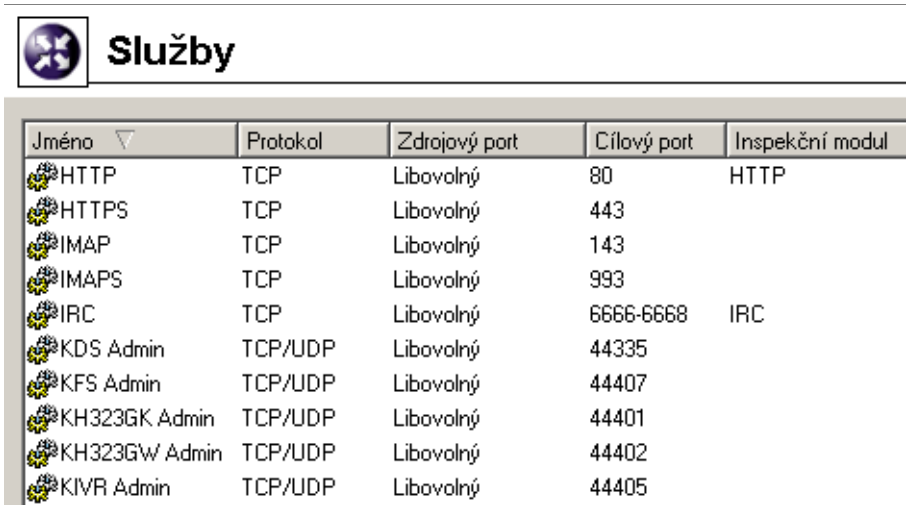
Poznámky:

1. Každý časový interval musí obsahovat alespoň jednu položku. Odebráním poslední položky časový interval zanikne.
2. Vytvořené časové intervaly nelze do sebe vnořovat.

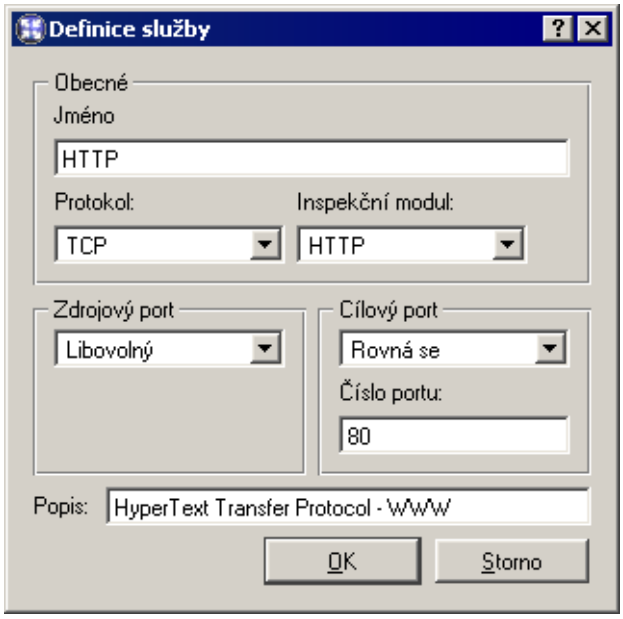
8.3 Služby

Služby ve *WinRoute* usnadňují definici komunikačních pravidel (povolení či zakázání přístupu z lokální sítě do Internetu nebo naopak zpřístupnění lokálního serveru z Internetu). Zjednodušeně lze říci, že služba je definována komunikačním protokolem a číslem portu, na kterém je přístupná (např. služba *HTTP* používá protokol TCP, port 80). K vybraným službám lze rovněž přiřadit inspekční modul (detaily viz dále).

Služby se definují v sekci *Konfigurace / Definice / Služby*. Ve výchozí instalaci *WinRoute* je zde již předdefinována řada standardních služeb (např. HTTP, FTP, DNS atd.).



Stisknutím tlačítka *Přidat* nebo *Změnit* se otevírá dialog pro definici služby.

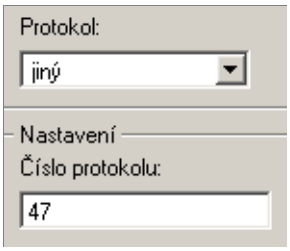


Jméno Identifikace služby v rámci *WinRoute*. Z důvodu přehlednosti by jméno mělo být stručné a výstižné.

Protokol Komunikační protokol, který služba používá.

Většina standardních služeb používá protokol *TCP* nebo *UDP*, případně oba (lze definovat jako jednu službu pomocí volby *TCP/UDP*). Další volby jsou *ICMP* (internetové řídicí zprávy) a *jiný*.

Volba *jiný* dovoluje specifikovat protokol jeho číslem v hlavičce IP paketu. Takto lze definovat libovolný protokol nesený v IP (např. GRE — číslo protokolu 47).



Inspekční modul Inspekční modul *WinRoute* (viz dále), který bude použit pro tuto službu.

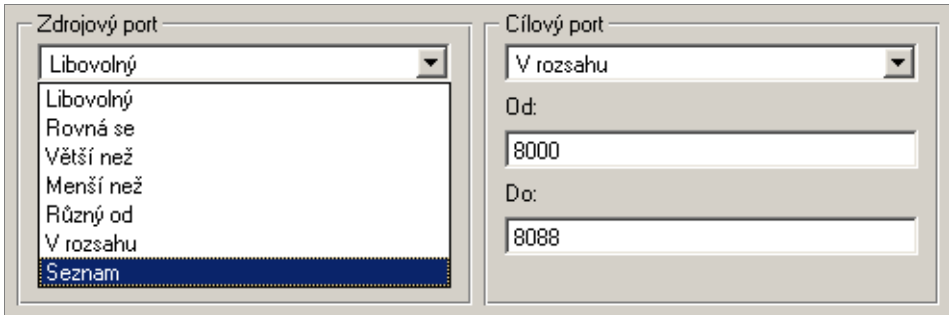
Upozornění: Každý modul by měl být používán pouze pro službu, pro kterou je určen. Použití nesprávného modulu pravděpodobně způsobí nefunkčnost dané služby.

Zdrojový a cílový port Je-li použit komunikační protokol TCP a/nebo UDP, pak je daná služba určena číslem cílového portu. Předpokládáme-li standardní model klient-

server, server čeká na spojení na známém portu (číslo odpovídá dané službě), zatímco klient svůj port předem nezná (bude mu přidělen operačním systémem při navazování spojení). Z toho vyplývá, že u standardních služeb je zpravidla znám cílový port, zatímco zdrojový může být (téměř) libovolný.

Poznámka: Specifikace zdrojového portu může mít význam např. při definici pravidla pro filtrování určitého typu komunikace. Podrobnosti najdete v kapitole 5.2.

Zdrojový a cílový port lze specifikovat jako:



- *Libovolný* — všechny porty (`1-65535`)
- *Rovná se* — konkrétní port (např. `80`)
- *Větší než*, *Menší než* — všechny porty s číslem větším, resp. menším než je zadáno
- *Různý od* — všechny porty kromě uvedeného
- *V rozsahu* — porty v zadaném rozsahu (včetně počátečního a koncového)
- *Seznam* — seznam portů oddělených čárkami (např.: `80,8000,8080`)

Popis Textový popis definované služby. Doporučujeme popisovat důsledně význam každé definice, zejména pokud se jedná o nestandardní služby — ušetříte si mnoho času a námahy při pozdějším odhalování chyb či předávání *WinRoute* jinému správci.

Inspekční moduly

WinRoute obsahuje speciální moduly, které sledují komunikaci daným aplikačním protokolem (např. HTTP, FTP apod.). Tuto komunikaci pak mohou určitým způsobem modi-

fikovat (filtrovat) nebo přizpůsobit chování firewallu danému protokolu. Výhody použití inspekčních modulů budou objasněny na dvou jednoduchých příkladech:

1. *Inspekční modul protokolu HTTP* sleduje komunikaci klientů (prohlížečů) s WWW servery a může blokovat přístup na určité stránky či stahování některých typů objektů (např. obrázky, reklamy či zvukové soubory).

2. Při použití FTP v aktivním režimu otevírá datové spojení server zpět na klienta. Za normálních okolností není možné přes firewall (resp. firewall s překladem adres) takovéto spojení navázat a FTP je možné používat pouze v pasivním režimu. *Inspekční modul FTP* však rozpozná, že se jedná o FTP v aktivním režimu a zajistí otevření příslušného portu a přesměrování spojení na odpovídajícího klienta v lokální síti. Uživatel v lokální síti pak není firewallem omezován a může používat FTP v obou režimech.

Inspekční modul se aktivuje, pokud je uveden v definici služby a tato služba použita v komunikačním pravidle. Je-li definováno pravidlo pro libovolnou službu, pak jsou pro komunikaci vyhovující tomuto pravidlu automaticky aktivní všechny inspekční moduly obsažené ve *WinRoute*. Každý inspekční modul obsluhuje protokol, pro který je určen, a službu, v jejíž definici je použit.

Poznámka: Inspekční moduly rozpoznávají aplikační protokoly na základě transportního protokolu (TCP nebo UDP) a čísla portu, který daná služba používá. Pokud služba běží na nestandardním portu (např. *HTTP* na portu 8080), pak nebude příslušným inspekčním modulem zpracována. Tuto situaci lze však jednoduše řešit definicí vlastní služby s použitím tohoto inspekčního modulu.

8.4 Skupiny URL

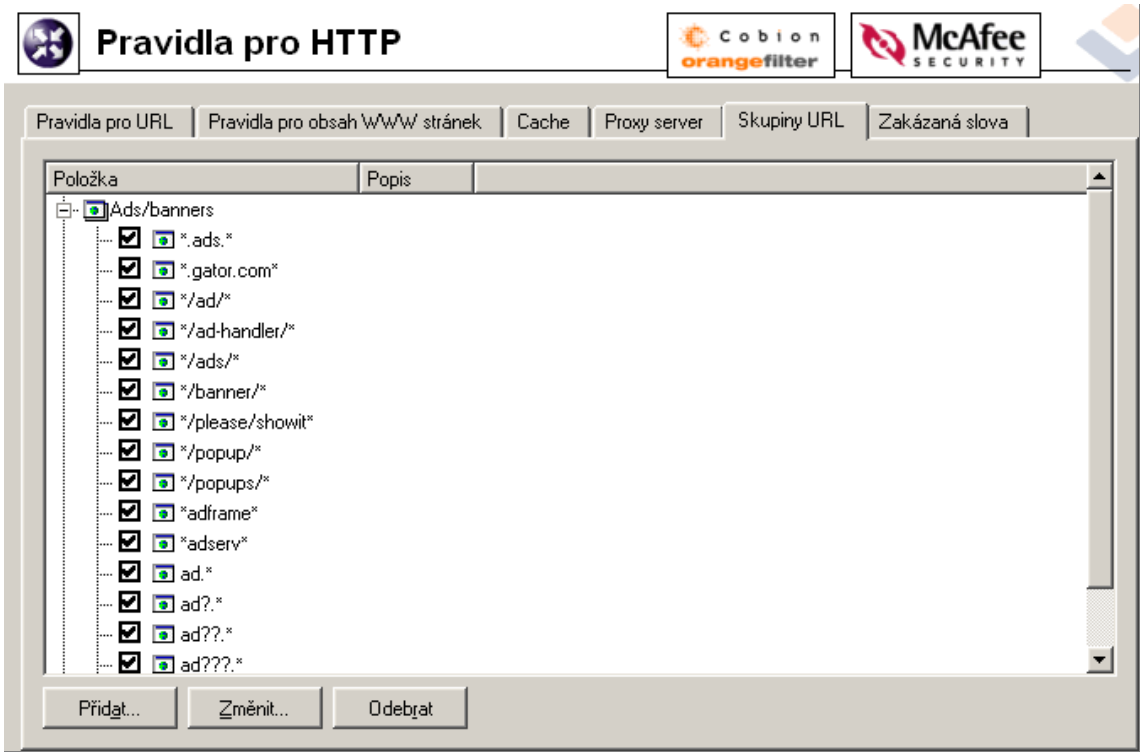
Skupiny URL slouží ke snadné a přehledné definici pravidel pro HTTP (viz kapitola 6.1). Chcete-li např. uživateli (či skupině uživatelů) zakázat přístup k určité skupině WWW stránek, není nutné vytvářet pro každou stránku pravidlo, stačí definovat skupinu URL a poté vytvořit jedno pravidlo pro tuto skupinu. Pravidlo pro skupinu URL je zpracováno podstatně rychleji, než velké množství pravidel pro jednotlivá URL.

Skupiny URL se definují v sekci *Konfigurace / Filtrování obsahu / Pravidla pro HTTP*, záložka *Skupiny URL*.

Zaškrtávací pole vedle každého URL slouží k jeho aktivaci a deaktivaci. Takto můžete URL dočasně vyřadit ze skupiny bez nutnosti jej odebírat a poté znovu přidávat.

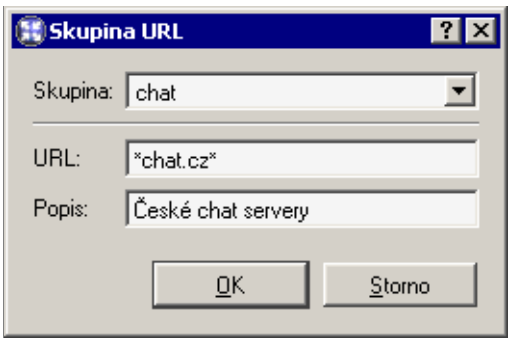
Poznámka: Výchozí instalace *WinRoute* obsahuje předdefinovanou skupinu URL:

- *Ads/Banners* typická URL stránek zobrazujících reklamy, reklamních pruhů na stránkách apod.



Správce *WinRoute* může tuto skupinu použít, případně upravit dle vlastního uvážení.

Po stisknutí tlačítka *Přidat* se zobrazí dialog, v němž lze vytvořit novou skupinu nebo přidat URL do již existující skupiny.



Skupina Jméno skupiny, kam má být URL přidáno. V této položce je možné:

- vybrat některou z existujících skupin
- zadat jméno nové (dosud neexistující) skupiny — tím dojde k vytvoření nové skupiny, do které bude zadané URL zařazeno.

URL URL, které má být do skupiny přidáno. Může být zadáno následovně:

- kompletní adresa serveru, dokumentu nebo stránky bez specifikace protokolu (`http://`)
- podřetězec se speciálními znaky `*` a `?`. Hvězdička nahrazuje libovolný počet znaků, otazník právě jeden znak.

Příklady:

- `www.kerio.cz/index.html` — konkrétní stránka
- `www.*` — všechna URL začínající `www.`
- `www.kerio.com` — všechna URL na serveru `www.kerio.com` (tento zápis je ekvivalentní výrazu `www.kerio.com/*`)
- `*sex*` — všechna URL obsahující řetězec `sex`
- `*sex??.cz*` — všechna URL obsahující řetězce typu `sexxx.cz`, `sex99.cz` atd.

Popis Textový popis významu zadan ého URL (pro snazší orientaci).

Kapitola 9

Uživatelské účty a skupiny

9.1 Uživatelské účty

Uživatelské účty v *WinRoute* slouží pro lepší řízení přístupu uživatelů z lokální sítě ke službám v Internetu. Uživatelský účet může být také použit pro přístup ke správě *WinRoute* pomocí programu *Kerio Administration Console*. Základní administrátorský účet se vytváří přímo během instalace *WinRoute*. Tento účet má plná práva pro správu *WinRoute* a může být odstraněn, pokud existuje alespoň jeden další účet s plnými právy ke správě.

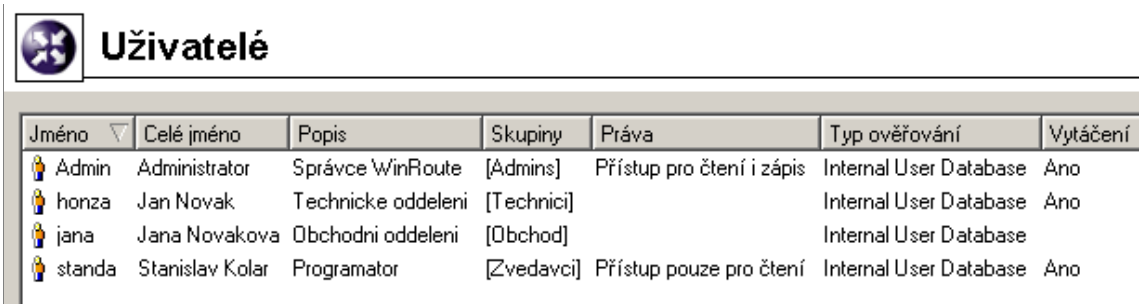
Upozornění:

1. Hesla k uživatelským účtům by měla být důsledně uchovávána v tajnosti, aby nemohlo dojít k jejich zneužití neoprávněnou osobou.

2. Odstraníte-li poslední účet s plnými právy ke správě a odhlásíte se z programu *Kerio Administration Console*, nebude již možné se ke správě *WinRoute* přihlásit. V tomto případě, stejně jako při zapomenutí administrátorského hesla, kontaktujte technickou podporu firmy *Kerio Technologies* (viz `http://www.kerio.cz/`).

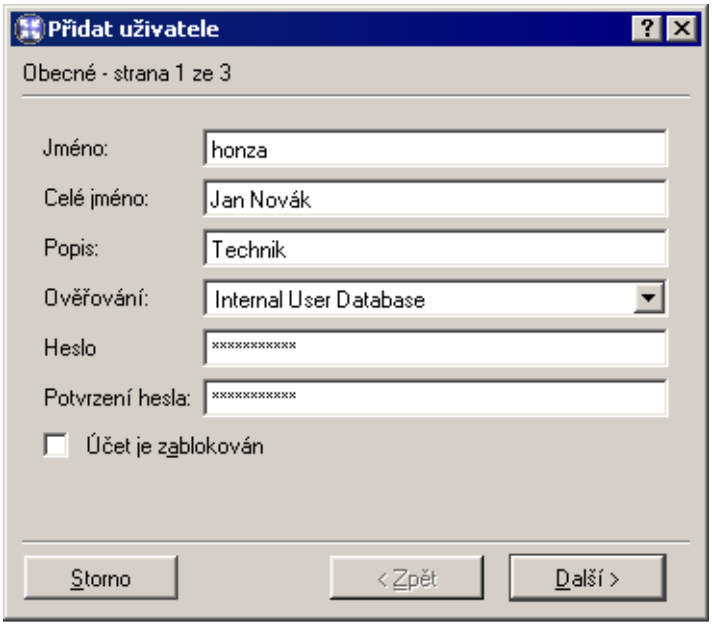
Vytvoření uživatelského účtu

Definice uživatelských účtů se provádí v sekci *Uživatelé a skupiny / Uživatelé*.



Stisknutím tlačítka *Přidat* se zobrazí průvodce vytvořením nového uživatelského účtu.

Krok 1 — základní údaje:



Jméno Přihlašovací jméno uživatele.

Upozornění: V uživatelském jméně se nerozlišují malá a velká písmena. Nedoporučuje se používat v uživatelském jméně české znaky (tj. písmena s diakritikou) — mohlo by dojít k problémům s přihlašováním pomocí WWW rozhraní.

Celé jméno Plné jméno (typicky jméno a příjmení daného uživatele)

Popis Textový popis uživatele (např. funkce)

Položky *Celé jméno* a *Popis* mají pouze informativní charakter. Mohou obsahovat libovolné informace nebo nemusejí být vyplněny vůbec.

Ověřování Způsob ověřování uživatele (viz dále)

Účet je zablokován Dočasné zrušení („vypnutí“) účtu bez nutnosti jej odstraňovat

Možné způsoby ověřování:

Interní databáze uživatelů Uživatel je ověřován pouze v rámci *WinRoute*. V tomto případě je potřeba zadat heslo do položek *Heslo* a *Potvrzení hesla* (své heslo pak může uživatel sám změnit pomocí WWW rozhraní — viz kapitola 7). Při tomto způsobu ověřování uživatelů nelze použít NTLM autentizaci.

Upozornění: Heslo smí obsahovat pouze tisknutelné znaky (písmena, číslice, interpunkční znaménka). V hesle se rozlišují malá a velká písmena. Nedoporučuje se používat v hesle české znaky (tj. písmena s diakritikou) — mohlo by dojít k problémům s přihlašováním pomocí WWW rozhraní.

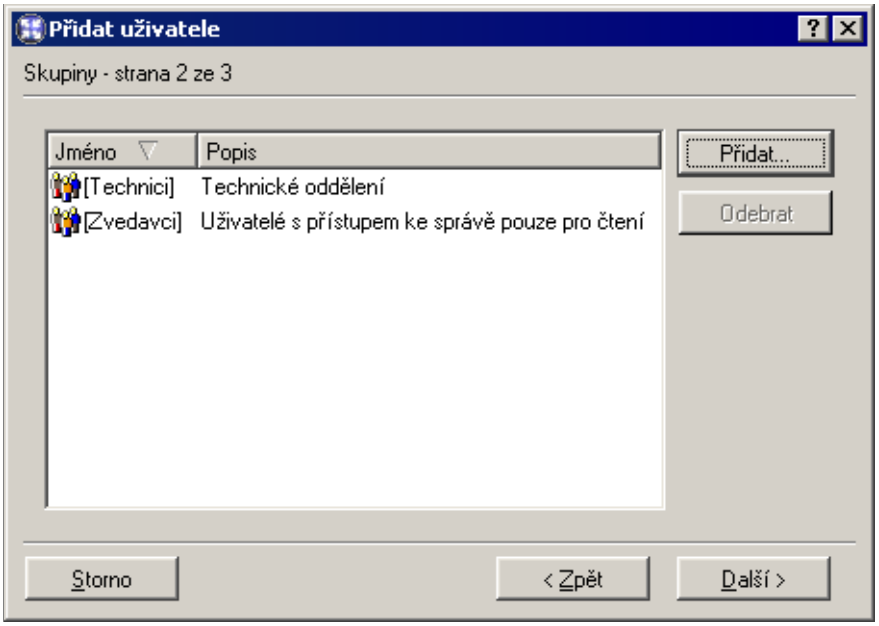
Doména Windows NT Uživatel bude ověřován v doméně Windows NT.

Tento způsob ověřování lze použít, pouze běží-li *WinRoute* na operačním systému Windows NT 4.0 / 2000 / XP.

Kerberos 5 Ověření uživatele přes ověřovací systém Kerberos verze 5. Tento způsob ověřování používá doména Windows 2000 (Active Directory).

Poznámka: NT doména a/nebo Kerberos 5 realm se nastavuje v sekci *Konfigurace / Další volby / Ověřování uživatele*. Podrobnosti naleznete v kapitole 7.2.

Krok 2 — skupiny:



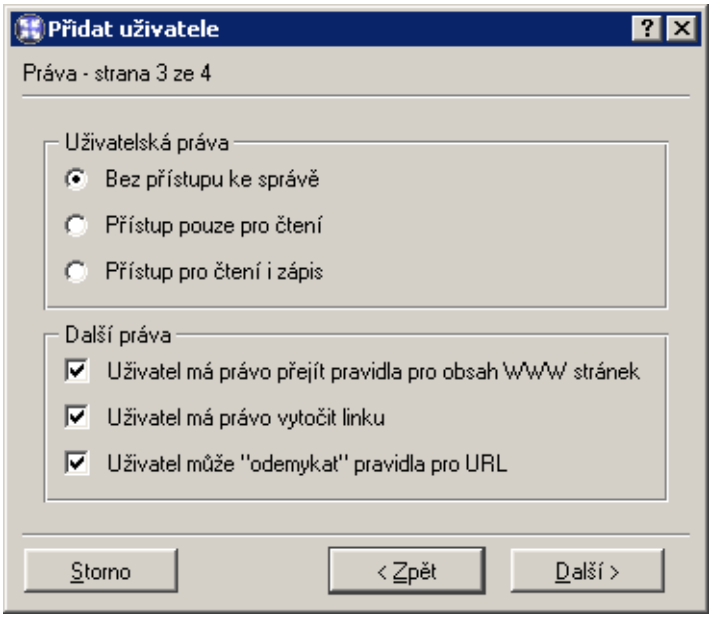
V tomto dialogu lze (tlačítky *Přidat* a *Odebrat*) přidat nebo odebrat skupiny, do kterých má být uživatel zařazen (skupiny se definují v sekci *Nastavení domény / Skupiny* — viz kapitola 9.2). Při definici skupin lze stejným způsobem do skupin přidávat uživatele — nezáleží na tom, zda budou nejprve vytvořeny skupiny nebo uživatelské účty.

Tip: Při přidávání skupin můžete označit více skupin najednou přidržením klávesy *Ctrl* nebo *Shift*.

Krok 3 — přístupová práva:

Každý uživatel musí mít nastavenu jednu ze tří úrovní přístupových práv.

Bez přístupu ke správě Uživatel nemá práva pro přihlášení ke správě *WinRoute*. Toto nastavení je typické pro většinu uživatelů — konfigurační úkony by měl provádět pouze jeden nebo několik správců.



Přístup pouze pro čtení Uživatel se může přihlásit ke správě *WinRoute*, může však pouze prohlížet záznamy a nastavení, nemá právo provádět žádné změny.

Přístup pro čtení i zápis Uživatel má plná práva ke správě, je ekvivalentní uživateli `Admin`. Existuje-li alespoň jeden uživatel s těmito právy, může být účet `Admin` odstraněn.

Doplňující volby:

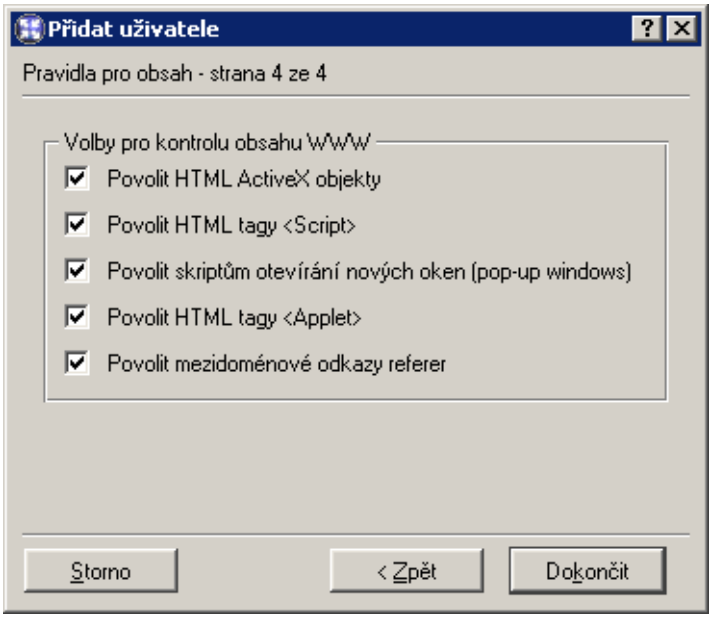
Uživatel má právo přejít pravidla... Tato volba umožňuje uživateli měnit osobní nastavení filtrování obsahu WWW stránek nezávisle na globálním nastavení (podrobnosti viz kapitoly 6.2 a 7.3).

Uživatel má právo vytočit linku Uživatel bude moci připojovat a zavěšovat vytáčené linky definované ve *WinRoute* (pomocí programu *Kerio Administration Console* nebo WWW administračního rozhraní — viz kapitola 7).

Uživatel může „odemykat“ pravidla pro URL Po zaškrtnutí volby je uživateli povoleno odemknout WWW stránky se zakázaným obsahem.

Krok 4 — pravidla pro kontrolu obsahu WWW stránek

Povolit HTML ActiveX objekty Prvky Microsoft ActiveX (bezpečnostní problémy v implementaci této technologie umožňují např. spouštění aplikací na klientském počítači).



Povolit HTML tagy <Script> HTML tagy `<script>` — příkazy jazyků JavaScript, VBScript atd.

Povolit skriptům otevírání nových oken Automatické otevírání nových oken prohlížeče — typicky reklamy.

Je-li tato volba vypnuta, pak *WinRoute* blokuje ve skriptech metodu `window.open()`.

Povolit HTML tagy <Applet> HTML tagy `<applet>` (*Java Applet*)

Povolit mezidoménové odkazy referer Položka `Referer` v HTTP hlavičce.

Tato položka obsahuje URL stránky, z níž klient na danou stránku přešel. Po vypnutí volby *Povolit mezidoménové odkazy referer* bude položka `Referer` blokována v případě, že obsahuje jiné jméno serveru než aktuální HTTP požadavek.

Blokování mezidoménových odkazů v položkách `Referer` má význam pro ochranu soukromí uživatele (položka `Referer` může být sledována pro zjištění, jaké stránky uživatel navštěvuje).

Úprava uživatelského účtu

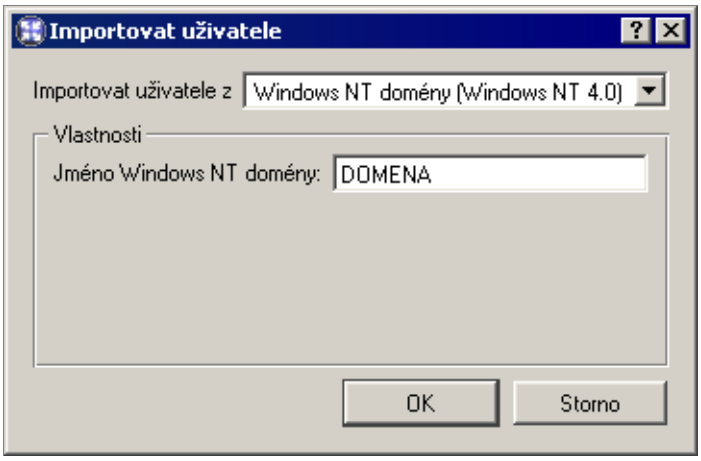
Tlačítko *Změnit* otevírá dialog pro změnu parametrů uživatelského účtu. Tento dialog obsahuje výše popsané části průvodce vytvořením účtu, uspořádané do záložek v jednom okně.

Import uživatelských účtů

Uživatelské účty mohou být nejen ručně definovány, ale mohou být také načteny z jiných zdrojů. K tomuto účelu slouží tlačítko *Importovat*. Volba *Importovat uživatele z* umožňuje vybrat zdroj, odkud mají být uživatelské účty převzaty:

NT doména (Windows NT 4.0) V tomto případě stačí uvést jediný parametr — *Jméno Windows NT domény*. Počítač, na kterém *WinRoute* běží, musí být členem do této domény.

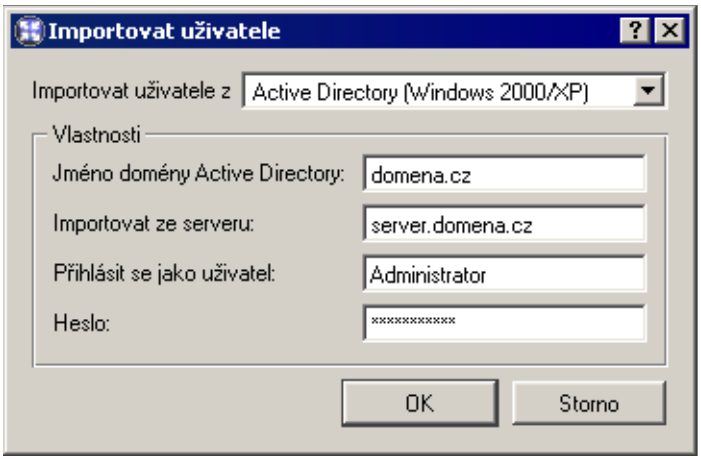
Upozornění: Nepoužívejte tento způsob importu uživatelských účtů, jestliže doménový server běží pod operačním systémem Windows 2000! V tomto případě vždy vyberte jako zdroj *Active Directory* — viz dále.

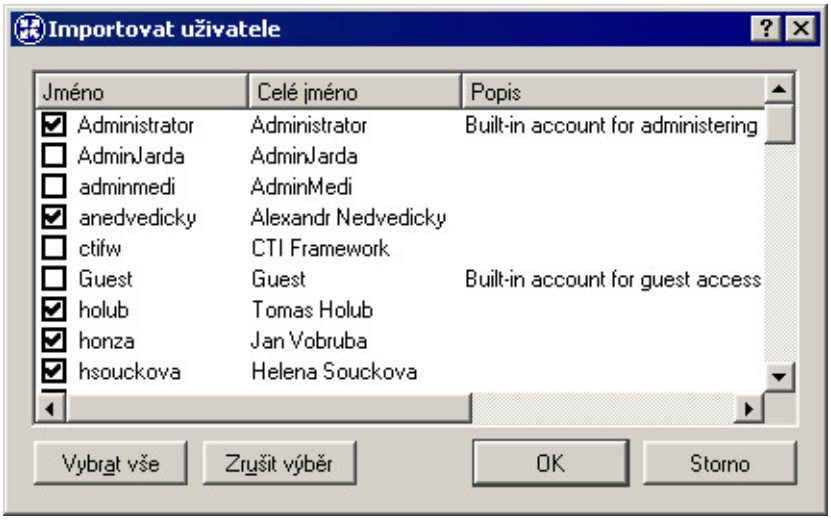


Active Directory (Windows 2000) Pro import uživatelských účtů z *Microsoft Active Directory* je třeba specifikovat následující údaje:

- *Jméno domény Active Directory* — název domény, z níž mají být uživatelské účty importovány (např. `domena.cz`).
- *Importovat ze serveru* — název doménového serveru *Active Directory* (např. `server.domena.cz`).
- *Přihlásit se jako uživatel*, *Heslo* — jméno a heslo uživatele, který má v této doméně vytvořen účet. Nejsou třeba žádná speciální uživatelská práva.

Pokud nedojde k chybě (byly zadány správné údaje, příslušný server je dostupný atd.), pak se po stisknutí tlačítka *OK* zobrazí seznam, z něhož lze zaškrtnutím vybrat uživatelské účty, které mají být do *WinRoute* přidány.





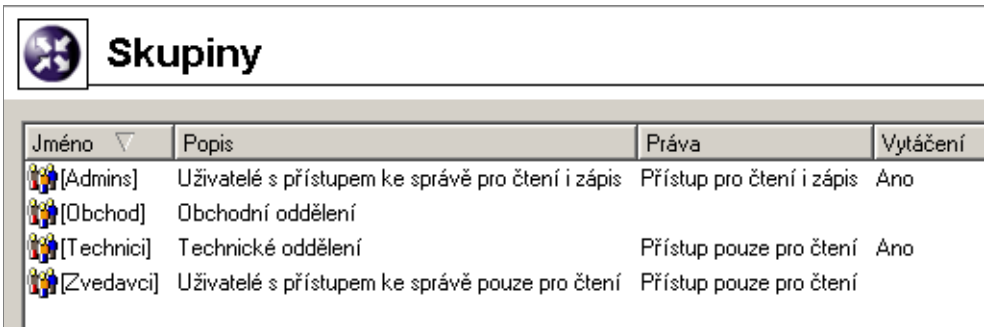
Jednotlivé uživatelské účty budou mít typ ověřování nastaven podle toho, odkud byly importovány: *Doména Windows NT* účty načtené z NT domény a *Kerberos 5* účty z *Active Directory* (*Active Directory* používá ověřovací systém *Kerberos 5*).

9.2 Skupiny uživatelů

Uživatelské účty lze řadit do skupin. Hlavní výhody vytváření skupin uživatelů jsou následující:

- Skupině uživatelů mohou být nastavena specifická přístupová práva. Tato práva doplňují práva jednotlivých uživatelů.
- Skupina může být použita při definici komunikačních či přístupových pravidel — definice se tím výrazně zjednoduší (není třeba definovat stejné pravidlo pro každého uživatele).

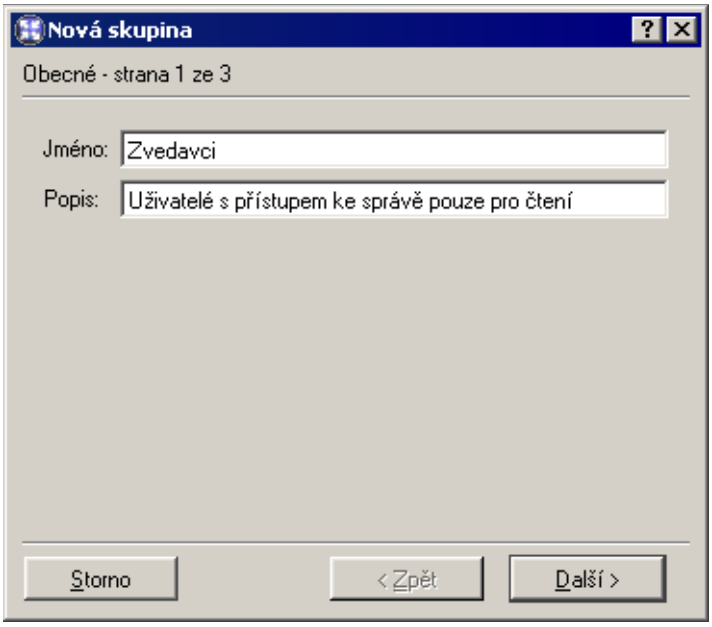
Skupiny uživatelů se definují v sekci *Uživatelé a skupiny / Skupiny*.



Vytvoření skupiny uživatelů

Novou skupinu uživatelů lze vytvořit tlačítkem *Přidat*. Po jeho stisknutí se zobrazí průvodce vytvořením skupiny uživatelů.

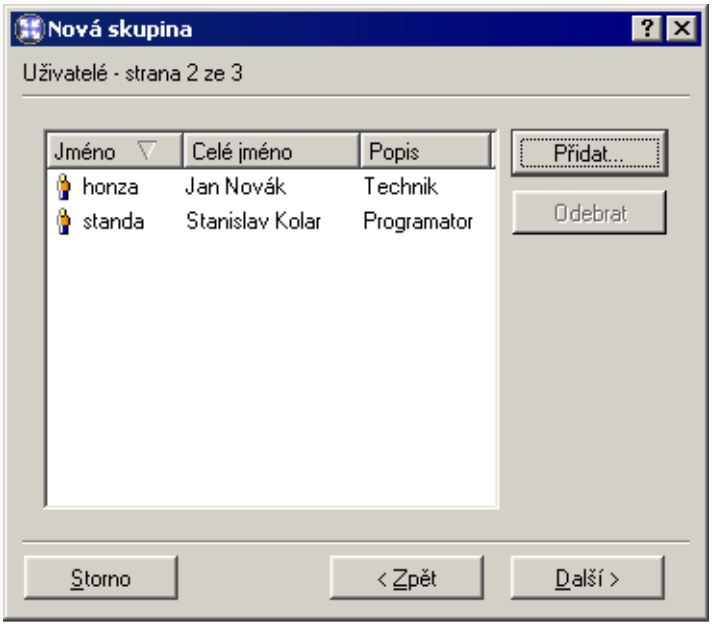
Krok 1 — název a popis skupiny:



Jméno Název skupiny (jednoznačně identifikuje skupinu)

Popis Textový popis skupiny (má pouze informativní charakter, může obsahovat libovolné informace nebo zůstat prázdný)

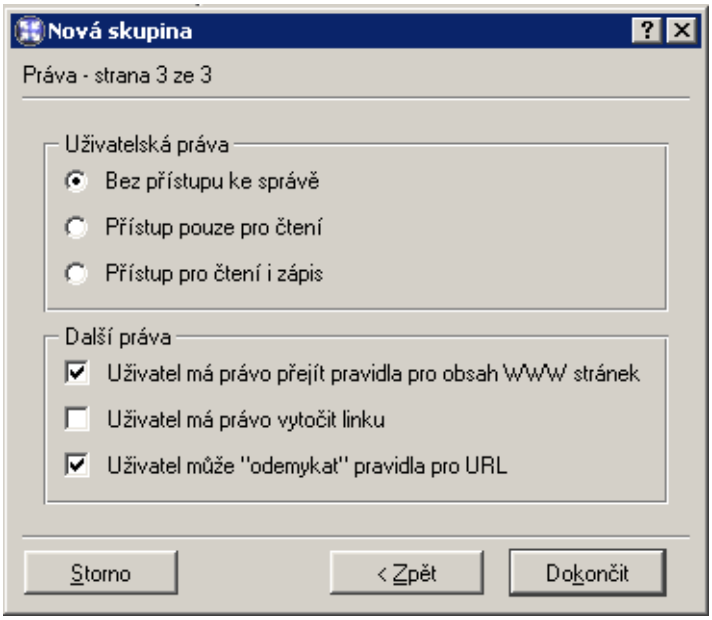
Krok 2 — členové skupiny



Tlačítky *Přidat* a *Odebrat* lze přidat či odebrat uživatele do/z této skupiny. Nejsou-li uživatelské účty dosud vytvořeny, může skupina zůstat prázdná a uživatelé do ní budou zařazeni při definici účtů (viz kapitola 9.1).

Tip: Při přidávání uživatelů lze označit více uživatelských účtů najednou přidržením klávesy *Ctrl* nebo *Shift*.

Krok 3 — přístupová práva skupiny



Skupina má vždy nastavenu jednu ze tří úrovní přístupových práv:

Bez přístupu ke správě Uživatelé v této skupině nemají práva pro přihlášení ke správě *WinRoute*.

Přístup jen pro čtení Uživatelé v této skupině se mohou přihlásit ke správě *WinRoute*, mohou však pouze prohlížet záznamy a nastavení, nemají právo provádět žádné změny.

Přístup pro čtení i zápis Uživatelé v této skupině mají plná práva ke správě.

Doplňující volby:

Uživatel má právo přejít pravidla... Tato volba umožňuje členům skupiny měnit osobní nastavení filtrování obsahu WWW stránek nezávisle na globálním nastavení (podrobnosti viz kapitoly 6.2 a 7.3).

Uživatel má právo vytočit linku Uživatelé zařazení v této skupině budou moci připojovat a zavěšovat vytáčené linky definované ve *WinRoute* (pomocí programu *Kerio Administration Console* nebo WWW administračního rozhraní — viz kapitola 7).

Uživatel může „odemykat“ pravidla pro URL Po zaškrtnutí volby je uživateli povoleno odemknout WWW stránky se zakázaným obsahem.

Přístupová práva skupiny se kombinují s vlastními právy uživatele — výsledná práva uživatele tedy odpovídají jeho vlastním právům a právům všech skupin, do kterých uživatelský účet patří.

Kapitola 10

Další nastavení

10.1 Nastavení vzdálené správy

Povolení či zákaz vzdálené správy se provádí definicí odpovídajícího komunikačního pravidla. Komunikace mezi *WinRoute* a programem *Kerio Administration Console* probíhá protokoly TCP a UDP na portu `44333`. Pro tento účel je ve *WinRoute* předdefinována služba *KWF Admin*.

Obsahuje-li *WinRoute* pouze komunikační pravidla vytvořená automaticky pomocí průvodce, pak je přístup ke vzdálené správě povolen přes všechna rozhraní s výjimkou toho, které je vybráno jako připojení do Internetu a je na něm aktivována funkce NAT (viz kapitola 5.1). Prakticky to znamená, že vzdálená správa je povolena ze všech počítačů v lokální síti.

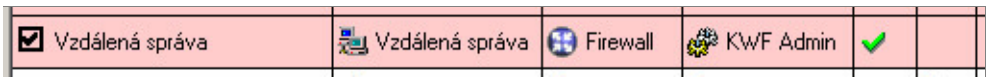
Povolení vzdálené správy z Internetu

Jako příklad uvedeme povolení vzdálené správy *WinRoute* z vybraných IP adres v Internetu.

- *Zdroj* — skupina IP adres, ze kterých má být vzdálená správa povolena.

  Z bezpečnostních důvodů nedoporučujeme povolovat vzdálenou správu z libovolného počítače v Internetu (tj. nastavovat jako *Zdroj* rozhraní připojené do Internetu)!

- *Cíl* — *Firewall* (tj. počítač, na němž *WinRoute* běží)
- *Služba* — *KWF Admin* (předdefinovaná služba — správa *WinRoute*)
- *Akce* — *Povolit* (jinak by vzdálená správa byla i nadále blokována)
- *Překlad* — nepřekládat zdrojovou ani cílovou adresu (tzn. nenastavovat žádný překlad adres)



Poznámka: Nesprávnou definicí komunikačního pravidla je možné zablokovat vzdálenou správu z počítače, z něhož ji právě provádíte. V takovém případě dojde k přerušení

spojení mezi *Kerio Administration Console* a *WinRoute Firewall Engine* (bezprostředně po stisknutí tlačítka *Použít* v sekci *Konfigurace / Komunikační pravidla*). Lokální připojení (tj. přímo z počítače, na němž běží *WinRoute Firewall Engine*) ale funguje vždy. Tuto komunikaci nelze zablokovat žádným pravidlem.

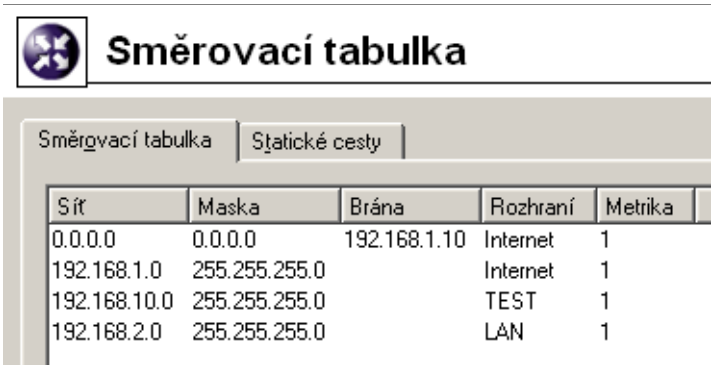
TIP: Obdobným způsobem lze ve *WinRoute* povolit či zakázat vzdálenou správu kteréhokoliv jiného produktu firmy Kerio Technologies — ve *WinRoute* jsou předdefinovány příslušné služby (např. *KMS Admin*, *KNM Admin* atd.).

10.2 Směrovací tabulka

V programu *Kerio Administration Console* můžete zobrazit a upravovat systémovou směrovací tabulku počítače, na němž *WinRoute* běží. Toto je velmi užitečné zejména při odstraňování problémů či úpravě konfigurace na dálku (není nutné používat aplikace pro terminálový přístup, sdílení pracovní plochy apod.).

K zobrazení a úpravě směrovací tabulky slouží sekce *Konfigurace / Směrovací tabulka*, která je rozdělena na dvě záložky:

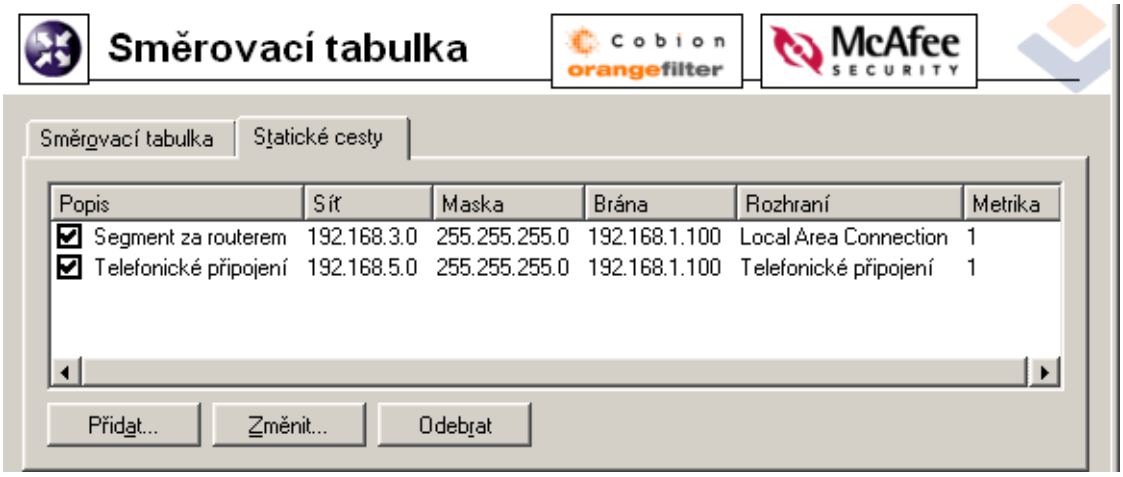
- *Směrovací tabulka* — aktuální směrovací tabulka operačního systému (včetně tzv. perzistentních cest v operačních systémech Windows 2000 a Windows XP).



  Zde je možné přidávat a rušit dynamické cesty. Přidaná dynamická cesta je platná pouze do restartu operačního systému, případně do odstranění systémovým příkazem `route`.

- *Statické cesty* — trvalé cesty, které *WinRoute* obnoví i po restartu operačního systému.

  WinRoute obsahuje speciální mechanismus pro vytváření a udržování statických cest ve směrovací tabulce. Veškeré cesty definované v záložce *Statické cesty* jsou uloženy do konfiguračního souboru a po každém startu *WinRoute Firewall Engine* vloženy do systémové směrovací tabulky. Po celou dobu běhu *WinRoute* jsou navíc tyto cesty



„hlídány“ — pokud někdo některou z nich příkazem `route` odstraní, *WinRoute* ji okamžitě opět přidá.

Poznámka: K implementaci statických cest nejsou využívány perzistentní cesty — tato funkce není k dispozici na všech operačních systémech.

Poznámka: Pokud zadáte do statické cesty rozhranní pro vytáčení (Telefonické připojení), pak paket směrovaný touto cestou způsobí vytočení linky (více v kapitole 10.3).

Upozornění: Jestliže je *WinRoute* spravován vzdáleně, může změna ve směrovací tabulce způsobit přerušení spojení mezi *WinRoute Firewall Engine* a *Kerio Administration Console* (bezprostředně po stisknutí tlačítka *Použít*). Doporučujeme upravenou směrovací tabulku vždy důkladně zkontrolovat!

Definice dynamických a statických cest

Po stisknutí tlačítka *Přidat* (resp. *Změnit* na vybrané cestě) se zobrazí dialog pro definici cesty.

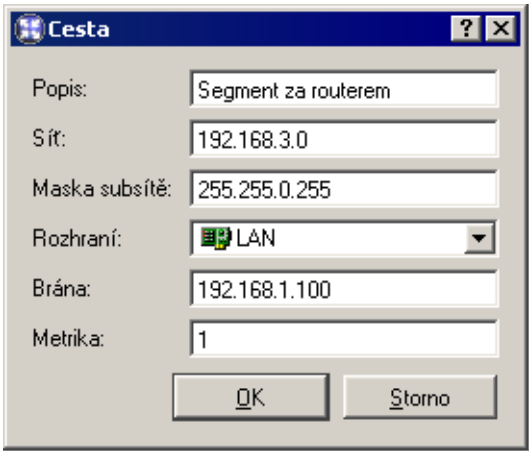
Popis Textový popis cesty (pro přehlednost). Tato položka je z technických důvodů k dispozici pouze v záložce *Statické cesty*.

Síť, Maska IP adresa a maska cílové sítě.

Rozhraní Výběr rozhraní, přes které budou pakety do uvedené sítě směrovány.

Brána IP adresa brány (směrovače), přes který vede cesta do cílové sítě (položka *Síť*). Adresa brány musí patřit do subsítě, do níž je připojeno zvolené rozhraní.

Metrika „Vzdálenost“ cílové sítě. Udává se v počtu směrovačů, přes které musí paket na této cestě projít.



Metrika slouží k určení nejlepší cesty do dané sítě — čím nižší metrika, tím „kratší“ cesta.

Poznámka: Metrika uvedená ve směrovací tabulce nemusí vždy odpovídat skutečné topologii sítě — může být např. upravena podle propustnosti jednotlivých linek apod.

Odstraňování záznamů ze směrovací tabulky

Pomocí administrační konzole *WinRoute* lze záznamy ze směrovací tabulky také mazat (tlačítkem *Odebrat*). Pro mazání cest platí následující pravidla:

- Cesty v záložce *Statické cesty* jsou plně v režii *WinRoute*. Zrušení cesty v této záložce znamená její okamžité a trvalé odebrání ze systémové směrovací tabulky (po stisknutí tlačítka *Použít*).
- Ručně definovaná dynamická cesta bude rovněž trvale odstraněna. Nezáleží na tom, zda byla přidána pomocí *Kerio Administration Console* nebo příkazem `route`.
- Perzistentní cesta bude ze směrovací tabulky rovněž odstraněna, ale pouze do restartu operačního systému. Po novém startu systému bude opět obnovena. Důvodem je, že existuje velmi mnoho způsobů, jak perzistentní cesty vytvářet (odlišné v každém operačním systému — např. příkazem `route -p`, příkazem `route` volaným z některého startovacího skriptu apod.). Technicky není možné zjistit, jakým způsobem je daná perzistentní cesta vytvořena a jak ji trvale zrušit.

10.3 Vytáčení na žádost

Je-li počítač s *WinRoute* připojen do Internetu vytáčenou linkou, vzniká zpravidla požadavek, aby bylo vytáčení a zavěšování linky určitým způsobem automatizováno (ruční

obsluha linky je většinou časově náročná a nepohodlná). *WinRoute* nabízí následující možnosti obsluhy vytáčené linky:

- Vytočení linky na základě požadavku z lokální sítě. Tato funkce se nazývá vytáčení na žádost a bude detailně popsána dále.
- Automatické zavěšení linky při nečinnosti, tj. pokud po ní nejsou po určitou dobu přenášena žádná data (ani v jednom směru). Popis nastavení automatického zavěšování vytáčené linky naleznete v kapitole 4.1.

Kdy a jak vytáčení na žádost funguje?

Prvním předpokladem vytáčení na žádost je, aby tato funkce byla zapnuta na příslušné lince (trvale nebo ve zvoleném časovém období). Toto nastavení se provádí v sekci *Konfigurace / Rozhraní* (detaily viz kapitola 4.1).

Druhou podmínkou je neexistence výchozí brány v operačním systému (tzn. na žádném síťovém adaptéru nesmí být definována výchozí brána). Tato podmínka se samozřejmě nevztahuje na vytáčenou linku, která má být pro přístup do Internetu použita — ta bude konfigurována dle informací od příslušného poskytovatele internetového připojení.

Jestliže *WinRoute* přijme z lokální sítě paket, porovnává jej se záznamy v systémové směrovací tabulce. Pokud se jedná o paket jdoucí do Internetu a linka je zavěšena, pak pro něj žádný odpovídající záznam nenalezne, protože ve směrovací tabulce neexistuje výchozí cesta. Za normálních okolností by byl paket zahozen a odesílateli vrácena řídicí zpráva, že cíl je nedostupný. Pokud je však zapnuta funkce vytáčení na žádost, *WinRoute* paket pozdrží ve vyrovnávací paměti a vytočí příslušnou linku. Tím dojde ve směrovací tabulce k vytvoření výchozí cesty, kudy je pak paket odeslán.

Od tohoto okamžiku výchozí cesta již existuje, a další pakety jdoucí do Internetu budou směrovány přes příslušnou linku (viz první případ). Linka pak může být zavěšena ručně nebo automaticky po nastavené době nečinnosti (příp. v důsledku chyby apod.). Dojde-li k zavěšení linky, odstraní se také výchozí cesta ze směrovací tabulky. Případný další paket do Internetu je opět podnětem pro vytočení linky.

Poznámky:

1. Pro správnou funkci vytáčení na žádost nesmí být nastavena výchozí brána na žádném síťovém adaptéru. Pokud by byla na některém rozhraní výchozí brána nastavena, pakety do Internetu by byly směrovány přes toto rozhraní (bez ohledu na to, kam je skutečně připojeno) a *WinRoute* by neměl žádný důvod vytáčet linku.
2. Pokud je ve *WinRoute* definováno více vytáčených linek, u nichž je povoleno automatické vytáčení na žádost, bude vždy vytáčena ta, která byla definována jako první. *WinRoute* neumožňuje automatický výběr linky, která má být vytočena.

3. Linka může být také vytáčena na základě statické cesty ve směrovací tabulce (viz kapitola 10.2). Je-li definována statická cesta přes vytáčenou linku, pak paket směrovaný touto cestou způsobí vytočení linky, jestliže je právě zavěšena. V tomto případě se ale přes tuto linku nevytváří výchozí cesta — nastavení *Použít výchozí bránu na vzdálené síti* (*Use default gateway on remote network*) v definici telefonického připojení je ignorováno.

4. V závislosti na faktorech, které ovlivňují celkovou dobu od přijetí podnětu do chvíle, kdy je linka vytočena (např. rychlost linky, doba potřebná pro vytočení atd.) může dojít k tomu, že klient vyhodnotí cílový server jako nedostupný (vyprší maximální doba pro přijetí odezvy) dříve, než je úspěšně navázáno spojení. *WinRoute* však požadavek na vytočení linky vždy dokončí. V takových případech stačí požadavek zopakovat (např. pomocí tlačítka *Obnovit* ve WWW prohlížeči).

Technická specifika a omezení

Vytáčení linky na žádost má určité specifické vlastnosti a principiální omezení. Ta je třeba mít na paměti zejména při návrhu a konfiguraci sítě, která má být připojena pomocí *WinRoute* a vytáčené linky do Internetu.

1. Vytáčení na žádost nefunguje přímo z počítače, na němž je *WinRoute* nainstalován. Technicky jej totiž realizuje nízkoúrovňový ovladač *WinRoute*, který pakety zachytává a dokáže rozhodnout, zda má být linka vytočena. Pokud je linka zavěšena a z lokálního počítače je vyslán paket do Internetu, pak je tento paket zahozen operačním systémem dříve, než jej může ovladač *WinRoute* zachytit.

2. Ve většině případů je při komunikaci klienta z lokální sítě se serverem v Internetu server odkazován DNS jménem. Proto zpravidla prvním paketem, který klient při komunikaci vyšle, je DNS dotaz pro zjištění IP adresy cílového serveru.

   Předpokládejme, že DNS server běží přímo na počítači s *WinRoute* (velmi častý případ) a linka do Internetu je zavěšena. Dotaz klienta na tento DNS server je komunikace v rámci lokální sítě a není tedy podnětem pro vytočení linky. Jestliže však DNS server nemá příslušný záznam ve své vyrovnávací paměti, musí dotaz předat jinému DNS serveru v Internetu. Nyní se jedná o paket vyslaný do Internetu aplikací, která běží přímo na počítači s *WinRoute*. Tento paket nelze zachytit a proto také nezpůsobí vytočení linky. V důsledku uvedených okolností nemůže být DNS dotaz vyřízen a v komunikaci nelze pokračovat.

   Pro tyto případy umožňuje *DNS Forwarder* ve *WinRoute* automatické vytočení linky, jestliže není schopen DNS dotaz sám vyřídit. Tato funkce je svázána s vytáčením na žádost — je-li vytáčení na žádost vypnuto, pak ani *DNS Forwarder* linku nevytáčí.

Poznámka: Bude-li DNS umístěn na jiném počítači v lokální síti nebo pokud budou klienti v lokální síti používat DNS server v Internetu, pak toto omezení neplatí a vytáčení na žádost bude fungovat normálně — v případě DNS serveru v Internetu způsobí vytočení linky přímo DNS dotaz klienta a v případě lokálního DNS serveru dotaz vyslaný tímto serverem do Internetu (počítač, na němž tento DNS server běží, musí mít nastavenu výchozí bránu na adresu počítače s *WinRoute*).

3. Z předchozího bodu vyplývá, že pokud má DNS server běžet přímo na počítači s *WinRoute*, musí to být *DNS Forwarder*, který dokáže v případě potřeby vytočit linku.

   Je-li v lokální síti Windows 2000 doména, která je založena na Active Directory, musí být použit Microsoft DNS sever, protože komunikace s Active Directory probíhá pomocí speciálních typů DNS dotazů. Microsoft DNS server však automatické vytáčení linky nepodporuje, a nemůže být ani nasazen na tomtéž počítači společně s *DNS Forwarderem*, protože by došlo ke kolizi portů.

   Z výše uvedeného vyplývá, že pokud má být připojení do Internetu realizováno vytáčenou linkou, *nemůže* být *WinRoute* nasazen na tentýž počítač, kde běží Windows 2000 server s Active Directory a Microsoft DNS.

4. Je-li použit *DNS Forwarder*, pak může za určitých okolností *WinRoute* vytáčet i na základě požadavku přímo z počítače, na němž je nainstalován.

   - Cílový server musí být zadán DNS jménem, aby aplikace generovala DNS dotaz.
   - V operačním systému musí být nastaven primární DNS „sám na sebe“ (tzn. na IP adresu některého interního rozhraní). V operačních systémech Windows to provedeme tak, že ve vlastnostech TCP/IP na některém z interních rozhraní nastavíme jako primární DNS stejnou IP adresu, jaká je přiřazena tomuto rozhraní.
   - *DNS Forwarder* musí předávat DNS dotazy některému ze zadaných DNS serverů (volba *Předávat dotazy těmto DNS serverům*) — nelze použít automatické zjišťování DNS serverů. Podrobnosti naleznete v kapitole 4.2.

Nastavení pravidel pro vytáčení na žádost

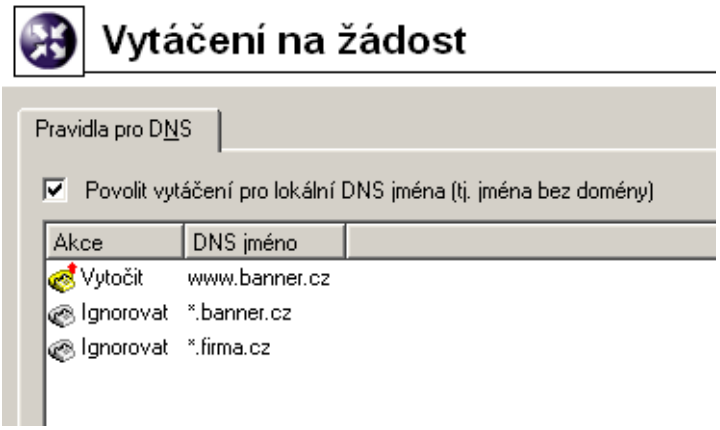
Vytáčení na žádost může mít v určitých případech nepříjemný postranní efekt — nechtěné vytáčení linky, zdánlivě bez zjevné příčiny. V naprosté většině případů je to způ-

sobeno DNS dotazy, které *DNS Forwarder* nedokáže zodpovědět, a proto vytočí linku, aby je mohl přeposlat na jiný DNS server. Typické jsou zejména následující situace:

- Počítač určitého uživatele generuje komunikaci, o níž uživatel neví. To může být např. reklamní banner na lokálně uložené HTML stránce či automatická aktualizace některého z instalovaných programů, ale také virus či trojský kůň.
- *DNS Forwarder* vytáčí na základě dotazů na jména lokálních počítačů. V tomto případě je třeba řádně nastavit DNS pro lokální doménu (k tomuto účelu postačí systémový soubor `hosts` na počítači, kde je *WinRoute* nainstalován — detaily viz kapitola 4.2).

Poznámka: Nežádoucí komunikaci je možné ve *WinRoute* blokovat, primární snahou by ale vždy mělo být odstranit její příčinu (tj. např. provést antivirovou kontrolu příslušné stanice apod.).

V sekci *Konfigurace / Vytáčení na žádost* programu *Kerio Administration Console* lze nastavit detailní pravidla pro vytáčení pro určitá DNS jména.



V této sekci se vytváří seřazený seznam pravidel pro DNS jména.

DNS jméno může být zadáno úplné, nebo jeho začátek či konec doplněn znakem hvězdička (*). Hvězdička nahrazuje libovolný počet znaků.

Akce může být *Vytočit* nebo *Ignorovat*, tj. nevytáčet při dotazu na toto DNS jméno.

Seznam pravidel je vždy procházen shora dolů (pořadí pravidel lze upravit tlačítky se šipkami na pravé straně okna). Při nalezení prvního pravidla, kterému dotazované DNS jméno vyhovuje, se vyhodnocování ukončí a provede se příslušná akce. Pro všechna DNS jména, pro něž nebude v seznamu nalezeno žádné vyhovující pravidlo, bude *DNS Forwarder* v případě potřeby automaticky vytáčet.

Akci *Vytočit* lze použít pro vytváření složitějších kombinací pravidel — např. pro jedno jméno v dané doméně má být vytáčení povoleno, ale pro všechna ostatní jména v této doméně zakázáno (viz příklad na obrázku).

Povolit vytáčení pro lokální DNS jména Lokální DNS jména jsou jména počítačů v dané doméně (tzn. jména, která neobsahují doménu).

Příklad: Lokální doména má název `firma.cz`. Počítač má název `pc1`. Jeho úplné doménové jméno je `pc1.firma.cz`, zatímco lokální jméno v této doméně je `pc1`.

Lokální jména jsou zpravidla uložena v databázi lokálního DNS serveru (v tomto případě v souboru `hosts` na počítači s *WinRoute*, který *DNS Forwarder* využívá). *DNS Forwarder* ve výchozím nastavení na tato jména nevytáčí, protože pokud není lokální jméno nalezeno v lokální DNS databázi, považuje se za neexistující.

V případech, kdy je primární server lokální domény umístěn mimo lokální síť, je třeba, aby *DNS Forwarder* vytáčel linku i při dotazech na tato jména. Toto zajistíme zapnutím volby *Povolit vytáčení pro lokální DNS jména* (v horní části okna *Vytáčení na žádost*).

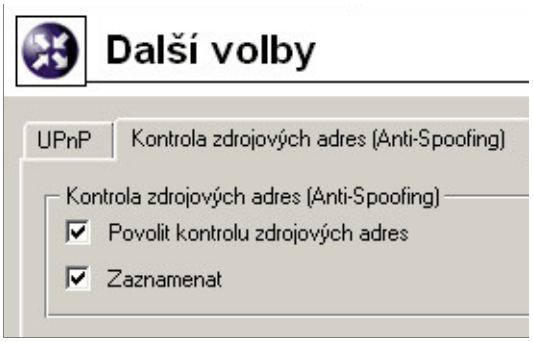
10.4 Kontrola zdrojových adres (Anti-Spoofing)

WinRoute umožňuje kontrolovat, zda na jednotlivá rozhraní počítače, na němž je nainstalován, přicházejí pouze pakety s přípustnými zdrojovými IP adresami. Tato funkce chrání počítač s *WinRoute* před útoky z vnitřní sítě za použití fiktivní IP adresy (tzv. *spoofing* — falšování IP adresy).

Z pohledu každého rozhraní je korektní taková zdrojová adresa, která patří do některé subsítě připojené k tomuto rozhraní (buď přímo, nebo přes další směrovače). Na rozhraní, přes které vede výchozí cesta (tj. rozhraní připojené do Internetu, též označováno jako externí rozhraní), je korektní libovolná IP adresa, která není povolena na žádném jiném rozhraní.

Přesnou informaci o tom, jaké subsítě jsou (přímo či nepřímo) připojeny k jednotlivým rozhraním, získává *WinRoute* ze systémové směrovací tabulky.

Konfigurace funkce *Anti-Spoofing* se provádí v sekci *Konfigurace / Další volby*, záložka *Kontrola zdrojových adres (Anti-Spoofing)*.



Povolit kontrolu zdrojových adres Tato volba zapíná výše popsanou funkci *Anti-Spoofing*.

Zaznamenat Po zapnutí této volby budou všechny pakety, které nevyhověly pravidlům kontroly zdrojových adres, zaneseny do záznamu *Security* (detaily viz kapitola 12.4).

10.5 Universal Plug-and-Play (UPnP)

WinRoute obsahuje podporu protokolu UPnP (*Universal Plug-and-Play*). Tento protokol umožňuje klientské aplikaci (např. *Microsoft Messenger*) detekovat firewall a vyžádat si otevření (mapování) potřebných portů na příslušný počítač. Toto mapování je vždy pouze dočasné — platí buď do uvolnění portů samotnou aplikací (pomocí zpráv protokolu UPnP) nebo do vypršení daného časového limitu.

Konfigurace UPnP se provádí v sekci *Konfigurace / Další volby*, záložka *UPnP*.

Povolit UPnP Zapnutí funkce *UPnP*.

Upozornění: Běží-li *WinRoute* na operačním systému Windows XP, pak se před zapnutím funkce *UPnP* přesvědčte, že nejsou spuštěny tyto systémové služby:

- *SSDP Discovery Service*
- *Universal Plug and Play Device Host*

Pokud ano, vypněte je a zakažte jejich automatické spuštění.

Tyto dvě služby obsluhují protokol UPnP ve Windows, a proto nemohou být spuštěny současně s funkcí *UPnP* ve *WinRoute*.

Časový limit pro mapování portů Porty, které daná aplikace požaduje, jsou z bezpečnostních důvodů vždy otevřeny (mapovány) pouze na určitou dobu. Mapování je automaticky zrušeno buď na požadavek aplikace, nebo po zadané době (v sekundách).

Protokol UPnP také umožňuje aplikaci otevření portů na dobu, o kterou si požádá. V tomto případě má parametr *Časový limit pro mapování portů* také význam maximální doby, na niž bude port aplikaci otevřen (pokud aplikace požádá o delší dobu, je automaticky zkrácena na tuto hodnotu).

Zaznamenat pakety Po zapnutí této volby budou do záznamu *Security* (viz kapitola 12.4) zaznamenány všechny pakety procházející přes porty mapované pomocí UPnP.

Zaznamenat spojení Po zapnutí této volby budou do záznamu *Connection* (viz kapitola 12.4) zaznamenána všechna spojení procházející přes porty mapované pomocí UPnP.

Upozornění: UPnP představuje nejen užitečnou funkci, ale také poměrně značnou bezpečnostní hrozbu — zejména v síti s velkým počtem uživatelů může dojít k téměř nekontrolovatelnému ovládání firewallu. Správce *WinRoute* by měl dobře zvážit, zda je důležitější bezpečnost nebo funkčnost aplikací vyžadujících UPnP.

Pomocí komunikačních pravidel (viz kapitola 5.2) je také možné omezit používání UPnP pouze z vybraných IP adres nebo pouze určitým uživatelům.

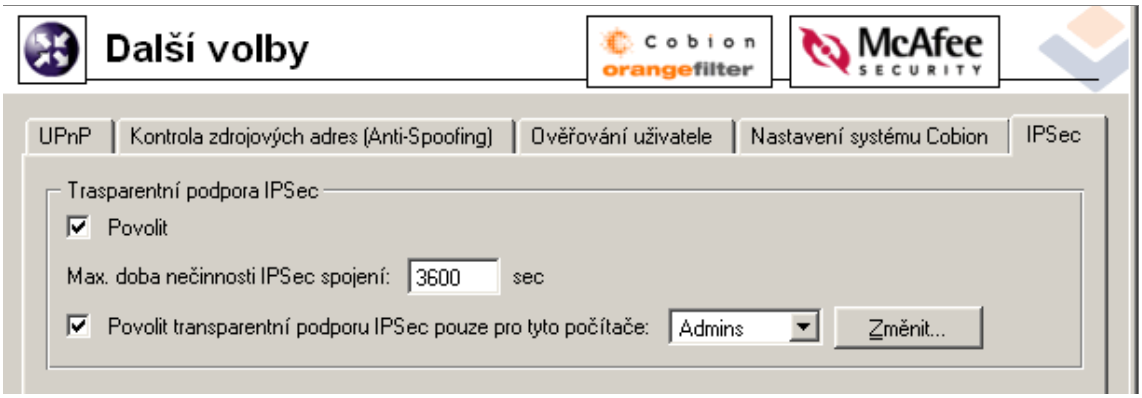
Příklad:

Jméno	Zdroj	Cíl	Služba	Akce
Povolení UPnP vybraným počítačům	Klienti UPnP	Firewall	UDP 1900 TCP 2168	✓
Zákaz UPnP	LAN	Firewall	UDP 1900 TCP 2168	✗

První pravidlo povolí používání UPnP pouze ze skupiny IP adres *Klienti UPnP*. Druhé pravidlo zakáže používání UPnP ze všech ostatních počítačů (IP adres).

10.6 Transparentní podpora IPsec

IPsec (IP Security Protokol) je rozšíření protokolu IP. Poskytuje šifrované bezpečnostní služby. Tyto služby dovolují autentizaci, kontrolu přístupu a důvěryhodnost. IPsec poskytuje podobné služby jako SSL, ale na síťové vrstvě. Přes IPsec lze vytvářet šifrované tunely (VPN) nebo jen šifruje komunikaci mezi dvěma počítači.



Povolit Volba umožňuje použití transparentní podpory IPsec.

Lze také nastavit maximální dobu nečinnosti IPsec spojení, po které může využít tento způsob spojení jiná IP adresa.

Povolit transparentní podporu IPsec ... Skupina IP adres, z nichž bude transparentní podpora IPsec povolena.

Kapitola 11

Registrace produktu a licence

Zakoupený produkt *Kerio WinRoute Firewall* je třeba zaregistrovat na WWW stránkách firmy Kerio Technologies (`http://www.kerio.cz/`). Registrací získáte licenční klíč (soubor s certifikátem `license.key`), který je třeba importovat do programu. Pokud tak neučiníte, bude se *WinRoute* chovat jako plně funkční, ale časově omezená verze.

Z výše uvedeného zároveň vyplývá, že rozdíl mezi zkušební verzí a plnou verzí *WinRoute* je pouze v tom, zda se do něj importuje licenční klíč či nikoliv. Každý zákazník má tak možnost si produkt ve třicetidenní lhůtě vyzkoušet v konkrétních podmínkách. Pokud si jej zakoupí a registruje, stačí pouze importovat získaný licenční klíč do nainstalované zkušební verze. Není tedy třeba *WinRoute* znovu instalovat a nastavovat.

V případě, že třicetidenní lhůta již vypršela, *WinRoute* zablokuje veškerou síťovou komunikaci počítače, na kterém je nainstalován. Povoleno je pouze přihlášení programem *Kerio Administration Console*, v němž pak lze importovat licenční klíč. Po importu platného licenčního klíče je *WinRoute* opět funkční v plném rozsahu.

11.1 Typy licencí

WinRoute může obsahovat volitelné moduly: antivirový program *McAfee* (viz kapitola 6.6) a systém hodnocení obsahu WWW stránek *Cobion Orange Filter* (viz kapitola 6.3). Tyto moduly jsou licencovány odděleně. Licenční klíč tedy obsahuje následující informace:

Licence *WinRoute* Základní licence *WinRoute*. Její platnost určují dvě data:

- skončení práva na aktualizaci — datum, do kdy je možné *WinRoute* bezplatně upgradovat na nejnovější verzi. Po tomto datu je *WinRoute* nadále funkční, ale nelze jej aktualizovat. Právo na aktualizaci můžete prodloužit zakoupením tzv. předplatného.

- skončení funkčnosti produktu — k tomuto datu přestává být *WinRoute* funkční a zablokuje veškerou TCP/IP komunikaci na počítači, kde je nainstalován. Pokud tato situace nastane, musíte importovat nový (platný) licenční klíč nebo *WinRoute* odinstalovat.

Licence antivirového programu *McAfee* Tato licence je určena dvěma daty:

- skončení práva na aktualizaci (nezávislé na *WinRoute*) — po tomto datu zůstává antivirus funkční, ale nelze aktualizovat virovou databázi ani antivirový program.

  Upozornění: Vzhledem ke stálému výskytu nových virů doporučujeme používat vždy nejnovější verzi virové databáze.

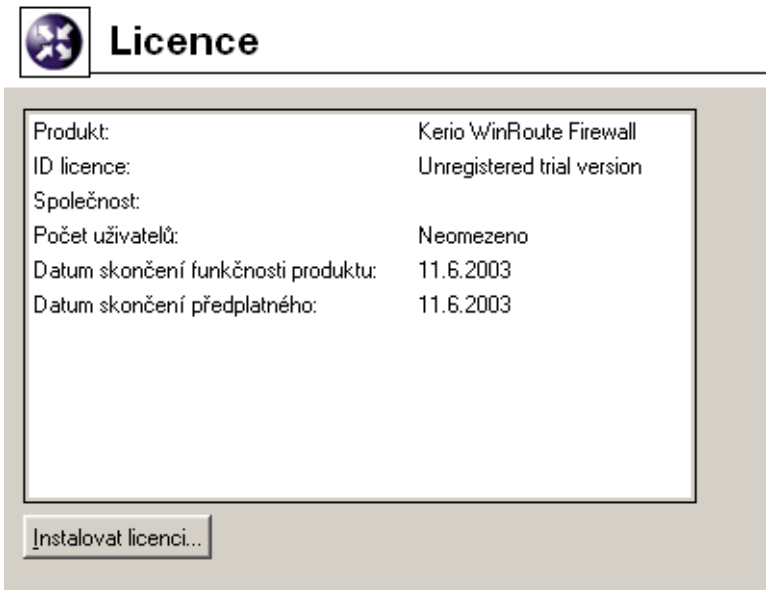
- skončení funkčnosti antivirového modulu — po tomto datu se antivirový modul *McAfee* zablokuje a nelze jej nadále používat.

Licence systému Cobion Orange Filter Systém *Cobion Orange Filter* je dodáván jako služba. Licence je určena pouze datem skončení platnosti, po kterém přestane systém *Cobion Orange Filter* fungovat.

Poznámka: Aktuální informace o jednotlivých licencích, možnostech prodloužení jejich platnosti atd. naleznete na WWW stránkách firmy Kerio Technologies (`http://www.kerio.cz/`).

11.2 Informace o licenci a import licenčního klíče

Informace o licenci lze zobrazit volbou *Konfigurace / Licence*.



Produkt Název produktu (*Kerio WinRoute Firewall*).

ID licence Licenční číslo.

Společnost Název společnosti (příp. osoby), na niž je produkt registrován.

Počet uživatelů Maximální počet počítačů (unikátních IP adres), které mohou současně přistupovat do Internetu. Tento počet nezahrnuje počítač s *WinRoute*.

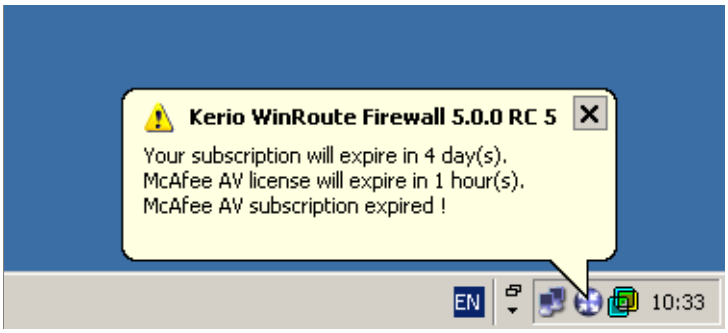
Datum skončení funkčnosti produktu Datum skončení funkčnosti produktu (pouze u zkušební verze nebo speciálních licencí).

Datum skončení předplatného Datum skončení nároku na bezplatný upgrade.

Tlačítko *Instalovat licenci* otevírá standardní dialog otevření souboru pro načtení souboru s licenčním klíčem. Je-li import úspěšný, zobrazí se informace o nové licenci.

11.3 Vypršení licence nebo práva na aktualizaci

Blíží-li se datum skončení platnosti licence *WinRoute*, antiviru *McAfee* nebo systému *Cobion Orange Filter* a/nebo skončení práva na aktualizaci *WinRoute* nebo antiviru *McAfee*, začne utilita *WinRoute Engine Monitor* periodicky zobrazovat informaci o tom, kolik dní zbývá do vypršení licence nebo skončení práva na aktualizaci.



Tato informace se poprvé zobrazí 7 dní před inkriminovaným datem a poté se zobrazuje periodicky několikrát denně až do chvíle, kdy přestane být *WinRoute* nebo některá z jeho komponent funkční, případě kdy skončí právo na aktualizaci *WinRoute* nebo antiviru *McAfee*.

Poznámka: Není-li spuštěn *WinRoute Engine Monitor*, nebude se tato informace zobrazovat.

11.4 Počítání a hlídání licencí

Pro počítání licencí si *WinRoute* udržuje tabulku s klienty, kteří komunikují do internetu. Každá unikátní IP adresa znamená jednu licenci (např. přihlášení k *WinRoute*). Licence se uvolňuje po 15 minutách nečinnosti klienta.

DNS dotazy, DHCP a lokální komunikace nejsou do licence započítávány.

Kapitola 12

Stavové informace a záznamy

WinRoute umožňuje správci (popř. jinému oprávněnému uživateli) poměrně detailně sledovat činnost firewallu. V podstatě se jedná o tři druhy informací: sledování stavu, záznamy a grafy.

- Sledovat lze komunikaci jednotlivých počítačů, přihlášené uživatele a spojení, která jsou přes *WinRoute* navázána.

  Poznámka: Zobrazuje se pouze komunikace, která je povolena komunikačními pravidly (viz kapitola 5). Pokud je zobrazena komunikace, o níž se domníváte, že by měla být zakázána, je třeba hledat chybu v pravidlech.

- Záznamy jsou soubory, do kterých se postupně přidávají informace o určitých událostech (např. chybová či varovná hlášení, ladicí informace atd.). Každá položka je zapsána na jedné řádce a uvozena časovou značkou (datum a čas, kdy událost nastala, s přesností na sekundy). Zprávy vypisované v záznamech jsou ve všech jazykových verzích *WinRoute* anglicky (vytváří je přímo *WinRoute Firewall Engine*).

- Grafy umožňují zobrazení časového průběhu zatížení jednotlivých rozhraní za vybrané časové období.

Jaké informace lze sledovat a jak lze přizpůsobit sledování potřebám uživatele je popsáno v následujících kapitolách.

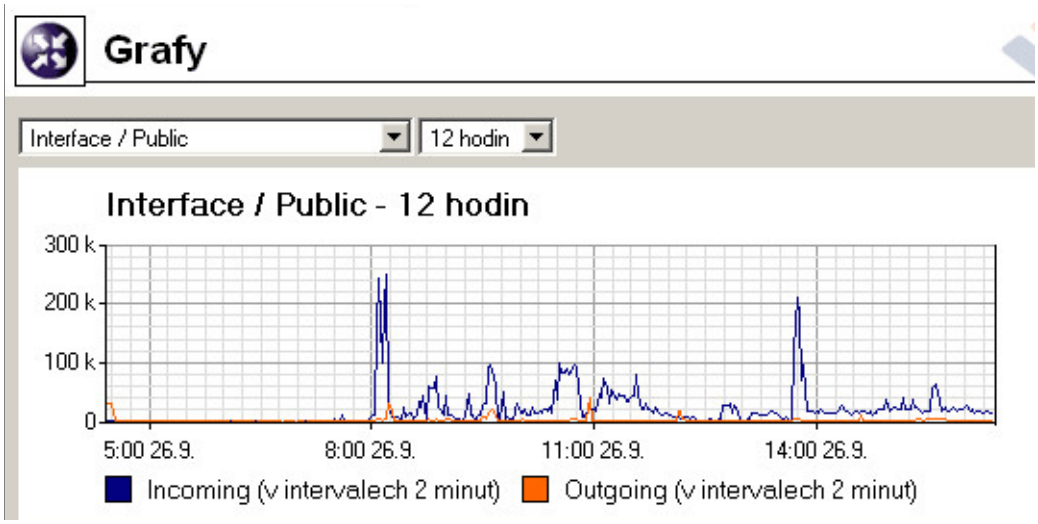
12.1 Grafy

V sekci *Stav / Grafy* může správce *WinRoute* graficky sledovat průběh zatížení jednotlivých síťových rozhraní (přenosovou rychlost v bytech za sekundu, *B/s*) za zvolené časové období.

Graf umožňuje nastavení následujících parametrů:

Sledované rozhraní První pole slouží pro výběr rozhraní, které má být sledováno. Ve výběru jsou nabídnuta všechna aktivní rozhraní (tj. aktivní síťové adaptéry a vytočené linky).

Časové období Ve druhém poli je možné vybrat časové období, ve kterém má být sledování prováděno (v rozsahu 2 hodiny — 30 dní). Zvolené časové období je vždy bráno od aktuálního času do minulosti („poslední 2 hodiny“, „posledních 30 dní“ apod.).



Komentář pod grafem zobrazuje interval vzorkování (t.j. interval, za který se hodnoty sečtou a zaznamenají do grafu).

Příklad: Je-li zvoleno časové období *2 hodiny*, provádí se vzorkování po 20 sekundách. To znamená, že se každých 20 sekund do grafu zaznamená průměrná přenosová rychlost za uplynulých 20 sekund.

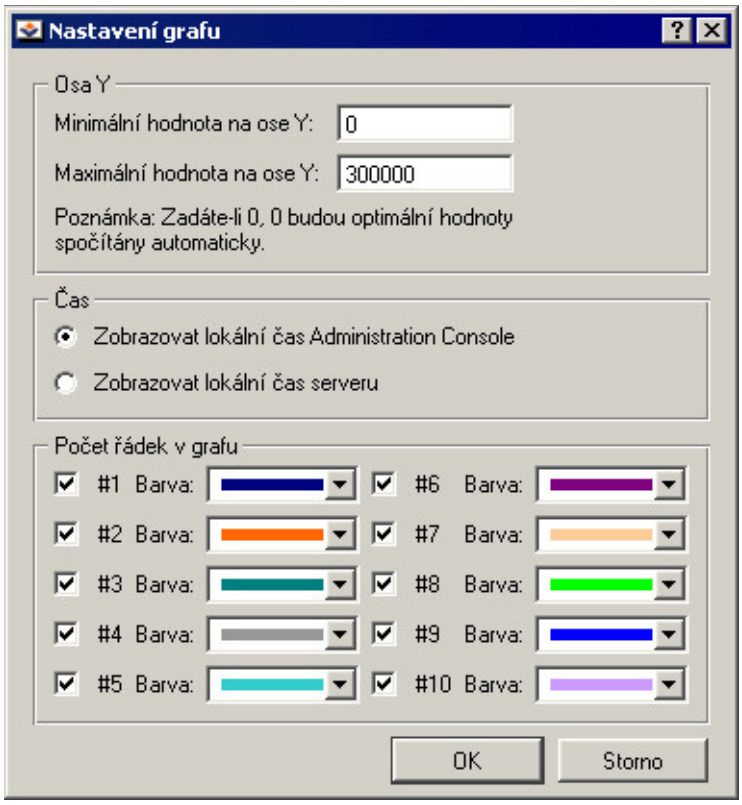
Tlačítko *Nastavení* otevírá dialog pro detailní nastavení vlastností grafu.

Osa Y Nastavení minimální a maximální hodnoty na ose *y*. Hodnota musí být zadána v základních jednotkách, v tomto případě v bytech — např. `100 KB` je třeba zadat jako `102400 (100*1024)`.

Poznámka: Měřítko osy *x* je pevně dáno vybraným časovým intervalem.

Čas Volba, který čas má být v grafu zobrazován (čas serveru nebo lokální čas počítače, na němž běží *Kerio Administration Console*). Obecně platí následující:

- Je-li *Kerio Administration Console* spuštěna přímo na počítači, kde je *WinRoute* nainstalován, jsou tyto časy vždy shodné.
- Totéž platí, pokud je čas na obou počítačích synchronizován (např. protokolem NTP či ve Windows NT doméně).
- Není-li čas synchronizován, ale oba počítače jsou ve stejném časovém pásmu, doporučujeme používat čas serveru.
- Je-li každý z těchto počítačů v jiném časovém pásmu, zvolte čas serveru nebo administrační konzoly podle potřeby.



Počet řádek v grafu Volba křivek, které mají být v grafu vykreslovány, a barev pro jejich zobrazování.

Poznámka: V grafu jsou vždy vykreslovány pouze křivky, které zvolená funkce generuje. Graf zatížení rozhraní ve *WinRoute* má pouze dvě křivky: #1 pro příchozí data a #2 pro odchozí data.

12.2 Počítače a uživatelé

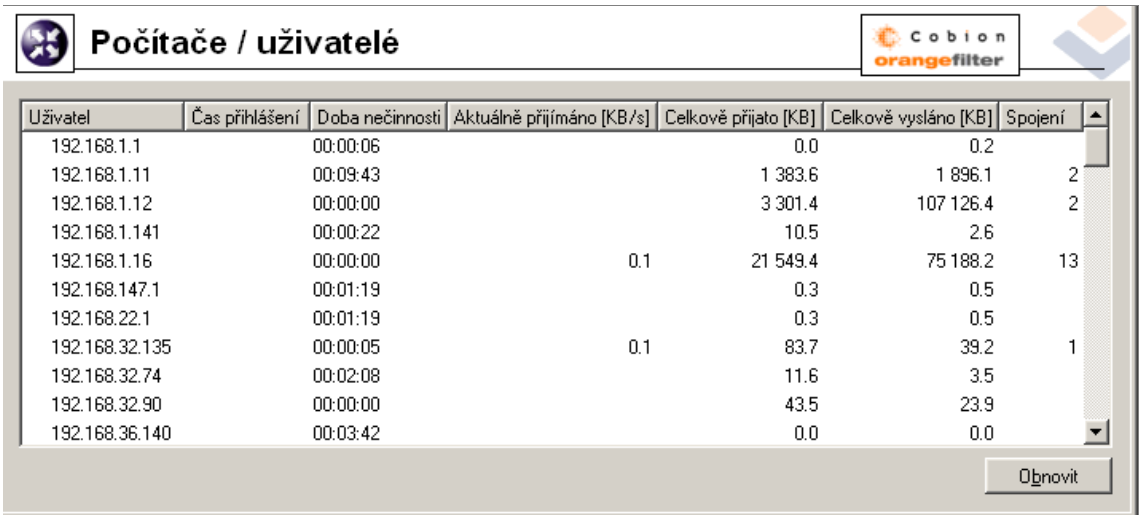
V sekci *Stav / Počítače / uživatelé* se zobrazují počítače z lokální sítě, případně přihlášení uživatelé, kteří komunikují přes *WinRoute* do Internetu.

Poznámka: Podrobnosti o přihlašování uživatelů na firewall naleznete v kapitole 7.2.

V okně *Počítače / uživatelé* mohou být zobrazeny následující informace:

Uživatel Tato položka může obsahovat:

- jméno uživatele přihlášeného k firewallu
- IP adresu počítače — jedná se o počítač, který přes *WinRoute* komunikuje, ale k firewallu z něj není přihlášen žádný uživatel



Uživatel	Čas přihlášení	Doba nečinnosti	Aktuálně přijímáno [KB/s]	Celkově přijato [KB]	Celkově vysláno [KB]	Spojení
192.168.1.1		00:00:06		0.0	0.2	
192.168.1.11		00:09:43		1 383.6	1 896.1	2
192.168.1.12		00:00:00		3 301.4	107 126.4	2
192.168.1.141		00:00:22		10.5	2.6	
192.168.1.16		00:00:00	0.1	21 549.4	75 188.2	13
192.168.147.1		00:01:19		0.3	0.5	
192.168.22.1		00:01:19		0.3	0.5	
192.168.32.135		00:00:05	0.1	83.7	39.2	1
192.168.32.74		00:02:08		11.6	3.5	
192.168.32.90		00:00:00		43.5	23.9	
192.168.36.140		00:03:42		0.0	0.0	

IP adresa IP adresa počítače, z něhož je uživatel přihlášen (resp. který komunikuje přes *WinRoute* s Internetem)

Čas přihlášení Datum a čas posledního přihlášení uživatele na firewall

Doba přihlášení Doba, po kterou je uživatel přihlášen (rozdíl aktuálního času a času přihlášení)

Doba nečinnosti Doba, po kterou daný počítač nepřenášel žádná data. Firewall může být nastaven tak, aby uživatele po určité době nečinnosti automaticky odhlásil (podrobnosti viz kapitola 7.1).

Počáteční čas Datum a čas, kdy byl daný počítač poprvé zaregistrován *WinRoute*. Tato informace se udržuje v operační paměti pouze po dobu běhu *WinRoute Firewall Engine*.

Aktuálně přijímáno, Aktuálně vysíláno Aktuální přenosová rychlost (v kilobytech za sekundu) v každém směru z pohledu daného počítače

Celkově přijato, Celkově vysláno Objem dat (v kilobytech) vyslaných a přijatých daným počítačem od *Počátečního času*

Spojení Celkový počet spojení z/na daný počítač. Volbou v kontextovém menu lze zobrazit detailní informace o těchto spojeních (viz dále).

Metoda ověření Ověřovací metoda použitá při posledním přihlášení uživatele:

- *plaintext* — uživatel se přihlásil na nezabezpečené přihlašovací stránce
- *SSL* — uživatel se přihlásil na přihlašovací stránce zabezpečené SSL

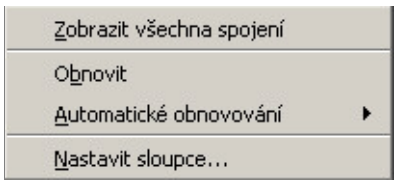
- *proxy* — uživatel přistupuje k WWW stránkám přes vestavěný proxy server, na němž se ověřil
- *NTLM* — uživatel byl automaticky ověřen v NT doméně pomocí NTLM (funguje při použití prohlížeče Microsoft Internet Explorer)

Detaily o přihlašování a ověřování uživatelů naleznete v kapitole 7.2.

Tlačítko *Obnovit* slouží k obnovení informací zobrazených v okně *Počítače / uživatelé*.

Volby pro okno Počítače / Uživatelé

Stisknutím pravého tlačítka myši v okně *Počítače / Uživatelé* (resp. přímo na vybraném záznamu) se zobrazí kontextové menu s následujícími volbami:



Zobrazit všechna spojení Tato volba otevře speciální okno, v němž jsou zobrazena veškerá spojení z/na vybraný počítač. Vzhled, chování a ovládání tohoto okna jsou zcela totožné s oknem *Stav / Spojení* (viz kapitola 12.3).

Poznámka: Tato volba je dostupná, pouze pokud bylo kontextové menu vyvoláno stisknutím pravého tlačítka myši na řádce s údaji o konkrétním počítači nebo uživateli. Pokud bylo pravé tlačítko stisknuto v ploše okna *Počítače / uživatelé* mimo zobrazené informace, je tato volba neaktivní.

Obnovit Okamžité obnovení informací v okně *Počítače / Uživatelé* (tato funkce je identická s funkcí tlačítka *Obnovit* pod oknem).

Automatické obnovování Nastavení automatického obnovování informací v okně *Počítače / Uživatelé*. Informace mohou být automaticky obnovovány v intervalu 5 sekund až 1 minuta nebo je možné automatické obnovování vypnout (*Neobnovovat*).

Nastavit sloupce Volba sloupců, která mají být v okně *Počítače / Uživatelé* zobrazeny (viz kapitola 3.6).

12.3 Zobrazení spojení

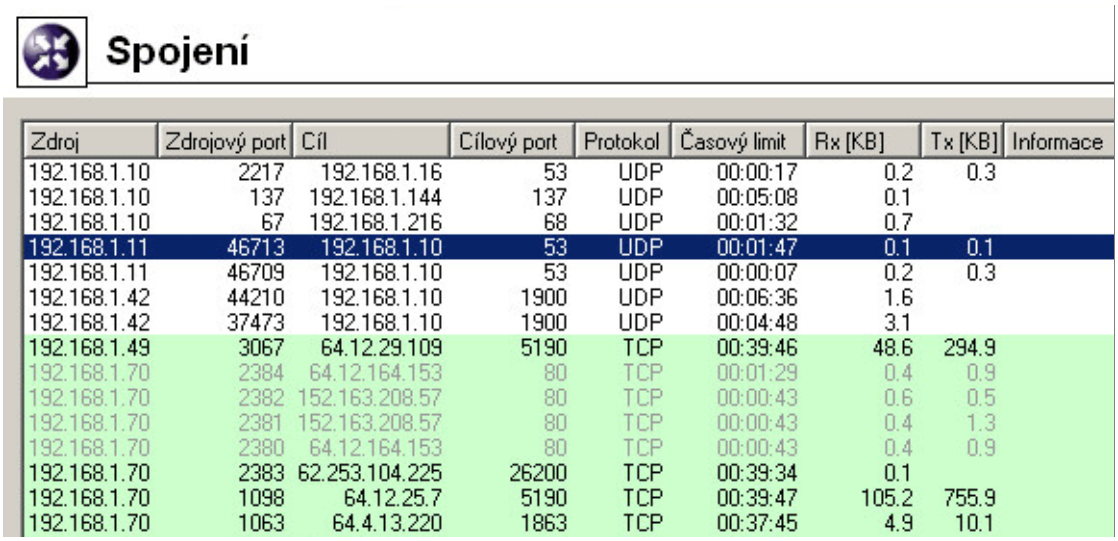
V sekci *Stav / Spojení* lze sledovat veškerá síťová spojení, která dokáže *WinRoute* zachytit, tzn.:

- spojení navázaná klienty přes *WinRoute* do Internetu
- spojení navázaná z počítače, na němž *WinRoute* běží
- spojení navázaná z jiných počítačů ke službám běžícím na tomto počítači
- spojení navázaná klienty v Internetu mapovaná na služby běžící v lokální síti

Poznámky:

1. *WinRoute* nezachytí (a tudíž nezobrazí) spojení navázaná mezi lokálními klienty.
2. Protokol UDP je tzv. nespojovaný protokol — nenavazuje žádné spojení, komunikace probíhá formou jednotlivých zpráv (tzv. datagramů). V tomto případě jsou sledována tzv. pseudospojení (periodická výměna zpráv mezi dvěma počítači je považována za jedno spojení).

Správce *WinRoute* může vybrané spojení „násilně“ ukončit.



Na každé řádce tohoto okna je zobrazeno jedno spojení. Jedná se o síťová spojení, nikoliv připojení uživatelů (každý klientský program může např. z důvodu rychlejší komunikace navázat více spojení současně). Sloupce zobrazují následující informace:

Zdroj, Cíl IP adresa zdroje (iniciátora spojení) a cíle. Pokud existuje v DNS příslušný reverzní záznam, zobrazuje se místo IP adresy odpovídající DNS jméno.

Zdrojový port, Cílový port Porty použité v daném spojení.

Protokol Komunikační protokol (*TCP* nebo *UDP*)

Časový limit Doba, za kterou bude spojení automaticky ukončeno. Tato doba se začne počítat od okamžiku, kdy přestanou být spojením přenášena data. Každý nový datový paket čítač této doby nuluje.

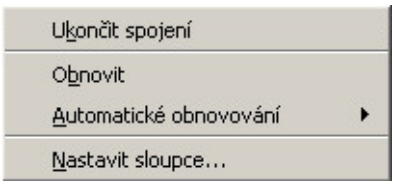
Rx, Tx Celkový objem dat přijatých (*Rx*) a vyslaných (*Tx*) v rámci tohoto spojení (v kilobytech). Vyslaná data jsou data přenášená směrem od *Zdroje* k *Cíli*, přijatá naopak.

Informace Textová informace o daném spojení (např. inspekční modul, který jej obsluhuje).

Informace v okně *Spojení* jsou automaticky obnovovány v nastaveném intervalu, navíc je také lze obnovit ručně tlačítkem *Obnovit*.

Volby pro okno Spojení

Stisknutím pravého tlačítka myši v okně *Spojení*, resp. přímo na vybraném spojení, se zobrazí kontextové menu s následujícími volbami:



Ukončit spojení Okamžité ukončení vybraného spojení (v případě UDP pseudospojení jsou zahazovány všechny následující datagramy).

Poznámka: Tato volba je dostupná pouze pokud bylo kontextové menu vyvoláno stisknutím pravého tlačítka myši na konkrétním spojení. Pokud bylo pravé tlačítko stisknuto v ploše okna *Spojení* mimo zobrazená spojení, je tato volba neaktivní.

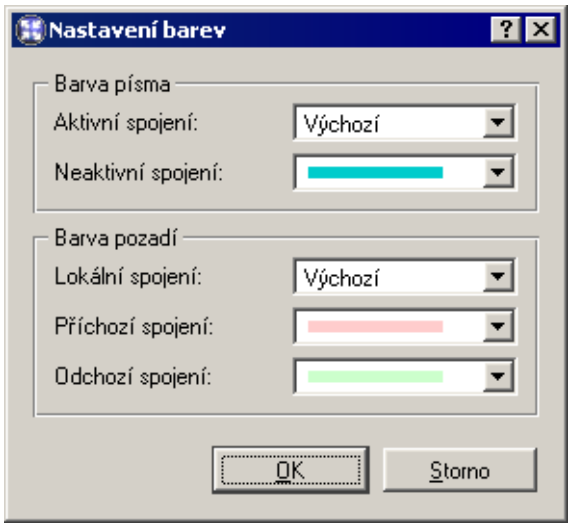
Obnovit Okamžité obnovení informací v okně *Spojení* (tato funkce je identická s funkcí tlačítka *Obnovit* pod oknem).

Automatické obnovování Nastavení automatického obnovování informací v okně *Spojení*. Informace mohou být automaticky obnovovány v intervalu 5 sekund — 1 minuta nebo je možné automatické obnovování vypnout (*Neobnovovat*).

Nastavit sloupce Volba sloupců, které mají být v okně *Spojení* zobrazeny (viz kapitola 3.6).

Nastavení barev

Tlačítko *Barvy* slouží k nastavení barev, kterými budou jednotlivá spojení zobrazována:



V každé položce je možné vybrat barvu nebo hodnotu *Výchozí*. Ta představuje barvu nastavenou v operačním systému (zpravidla černá pro text a bílá pro pozadí).

Barva písma

- *Aktivní spojení* — spojení, jimiž jsou aktuálně přenášena data
- *Neaktivní spojení* — TCP spojení, která byla ukončena, ale jsou dosud udržována (standard stanoví, že spojení musí být udržováno ještě 2 minuty po jeho ukončení — z důvodu opakovaného vysílání chybných paketů)

Barva pozadí

- *Lokální spojení* — spojení, jejichž zdrojem nebo cílem je některá z IP adres počítače s *WinRoute*
- *Příchozí spojení* — spojení navázaná z Internetu do lokální sítě (povolená firewallem)
- *Odchozí spojení* — spojení navázaná z lokální sítě do Internetu

Poznámka: Rozlišení příchozích a odchozích spojení se provádí podle toho, jakým směrem probíhá překlad IP adres — „ven“ (*SNAT*) nebo „dovnitř“ (*DNAT*). Detaily naleznete v kapitole 5.

12.4 Záznamy

Záznamy jsou soubory uchovávající zprávy o vybraných událostech, k nimž ve *WinRoute* došlo, nebo které *WinRoute* zachytil.

Každý záznam je zobrazován v jednom okně v sekci *Záznamy*. Každý řádek každého záznamu obsahuje informaci o jedné události. Řádek vždy začíná časovou značkou v hranatých závorkách (datum a čas, kdy událost nastala, s přesností na sekundy). Za ní následuje konkrétní informace (v závislosti na typu záznamu).

Fyzicky jsou záznamy uloženy v souborech v podadresáři `logs` adresáře, kde je *WinRoute* nainstalován. Jména těchto souborů mají formát:

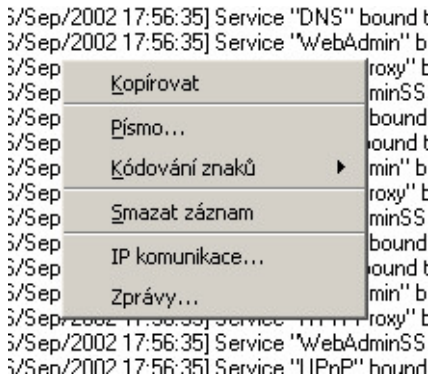
```
název_záznamu.log
```

(např. `debug.log`). Ke každému záznamu přísluší také soubor s příponou `.idx`, což je indexový soubor pro rychlejší přístup do záznamu při jeho zobrazování v *Kerio Administration Console*.

Uložení záznamů v souborech umožňuje zálohování záznamů (zkopírováním do jiného adresáře), nebo jejich zpracování různými analytickými nástroji.

Nastavení záznamů

V okně každého záznamu se po stisknutí pravého tlačítka myši zobrazí kontextové menu, v němž lze zvolit různé funkce nebo změnit parametry záznamu (zobrazení, příp. sledované informace).



Nastavení záznamu Volba je dostupná pouze u záznamů *http* a *web*.

Volba umožňuje povolit nebo zakázat zápis záznamu.

Kopírovat Zkopírování označeného textu do schránky (clipboardu). Pro tuto funkci lze využít také klávesové zkratky operačního systému (např. ve Windows *Ctrl-C* nebo *Ctrl-Insert*).

Písmo Dialog výběru písma pro výpis záznamu. K dispozici jsou všechna písma instalovaná na počítači, kde je spuštěna *Kerio Administration Console*.

Kódování znaků Výběr kódování, které bude použito pro zobrazení záznamu v programu *Kerio Administration Console*. Výchozí kódování je *UTF-8*.

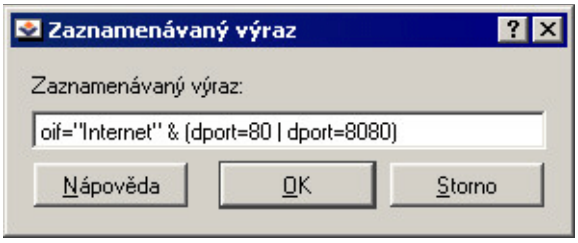
TIP: Pokud se v záznamu nezobrazují korektně české znaky, zkuste zvolit jiné kódování.

Smazat záznam Smazání celého záznamu. Tato volba smaže celý soubor záznamu (nikoliv pouze část zobrazenou v aktuálním okně).

Upozornění: Smazaný záznam již nelze obnovit!

Následující volby jsou dostupné pouze v záznamu *Debug*:

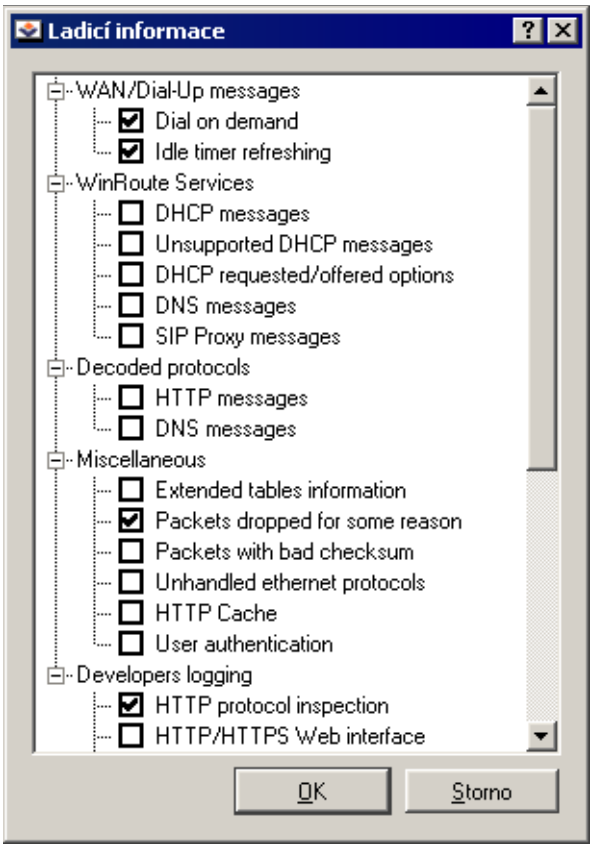
IP komunikace Sledování paketů na základě zadaného výrazu.



Výraz je třeba zapsat speciální symbolikou (obdoba zápisu podmínky v programovacím jazyce). Stisknutím tlačítka *Nápověda* se zobrazí stručný popis možných podmínek a příklady jejich použití.

Zprávy Možnost detailního nastavení informací, které mají být sledovány:

- *WAN / Dial-up messages* — informace o vytáčených linkách (vytáčení na žádost, čítač doby automatického zavěšení)
- *WinRoute services* — činnost služeb *WinRoute* (DHCP server, DNS forwarder, SIP proxy)
- *Decoded protocols* — zobrazení obsahu zpráv vybraných protokolů, které jsou obsluhovány moduly *WinRoute* (HTTP a DNS)
- *Miscellaneous* — různé další informace (např. zahozené pakety, pakety s chybami, HTTP cache, ověřování uživatelů...)
- *Developers logging* — detailní záznamy pro účely ladění (lze použít např. při řešení problémů s technickou podporou)



Záznam Config

Záznam *Config* uchovává kompletní historii komunikace *Kerio Administration Console* s *WinRoute Firewall Engine* — z tohoto záznamu lze zjistit, který uživatel kdy prováděl jaké administrační úkony.

Příklad záznamů v okně Config:

```
[18/Apr/2003 10:25:02] standa - session opened
 for host 192.168.32.100
[18/Apr/2003 10:27:46] standa - insert StaticRoutes
 set Enabled='1', Description='VPN',
 Net='192.168.76.0', Mask='255.255.255.0',
 Gateway='192.168.1.16', Interface='LAN', Metric='1'
```

```
[18/Apr/2003 10:32:56] standa - session closed
 for host 192.168.32.100
```

- `[18/Apr/2003 10:25:02]` — datum a čas, kdy byl záznam zapsán
- `standa` — jméno uživatele přihlášeného ke správě *WinRoute*
- `session opened for host 192.168.32.100` — informace o zahájení komunikace a IP adrese počítače, ze kterého je *Kerio Administration Console* k *WinRoute Firewall Engine* připojena
- `insert StaticRoutes ...` — vložení záznamu do konfigurační databáze *WinRoute* (v tomto případě přidání statické cesty do směrovací tabulky)
- `session opened for host 192.168.32.100` — informace o ukončení komunikace s daným počítačem (odhlášení uživatele nebo ukončení *Kerio Administration Console*)

Záznam Connection

Záznam spojení odpovídajících komunikačním pravidlům, u nichž byla zapnuta volba *Zaznamenat odpovídající spojení* (viz kapitola 5).

Jak číst záznam Connection?

```
[18/Apr/2003 10:22:47] [ID] 613181 [User] standa
[Connection] TCP 192.168.1.140:1193 -> hit.navrcholu.cz:80
[Duration] 121 sec [Bytes] 1575/1290/2865 [Packets] 5/9/14
```

- `[18/Apr/2003 10:22:47]` — datum a čas, kdy byl záznam zapsán (pozn.: záznam o spojení se ukládá bezprostředně po ukončení příslušného spojení)
- `[ID] 613181` — identifikátor spojení ve *WinRoute*
- `[User] standa` jméno uživatele přihlášeného k firewallu z počítače, který se účastní komunikace (není-li z tohoto počítače přihlášen žádný uživatel, zobrazuje se zde `<null>`)
- `[Connection] TCP 192.168.1.140:1193 -> hit.navrcholu.cz:80` — protokol, zdrojová IP adresa a port, cílová IP adresa a port. Je-li v cache *DNS Forwarderu* (viz kapitola 4.2) nalezen odpovídající záznam, zobrazí se namísto IP adresy DNS jméno počítače. Není-li záznam v cache nalezen, jméno počítače se nezjišťuje (dotazování DNS by příliš zpomalovalo činnost *WinRoute*).

- `[Duration] 121 sec` — doba trvání spojení (v sekundách)
- `[Bytes] 1575/1290/2865` — počet bytů přenesených tímto spojením (vysláno/přijato/celkem)
- `[Packets] 5/9/14` — počet paketů přenesených tímto spojením (vysláno/přijato/celkem)

Záznam Debug

Debug (ladicí informace) je speciální záznam, který slouží k detailnímu sledování určitých informací, zejména při odstraňování problémů. Těchto informací je poměrně velké množství, což by způsobilo naprostou nepřehlednost tohoto záznamu, pokud by byly zobrazovány všechny současně. Zpravidla je však třeba sledovat pouze informace týkající se konkrétní služby či funkce. Zobrazování velkého množství informací navíc zpomaluje činnost *WinRoute*. Doporučujeme tedy zapínat sledování pouze těch informací, které vás skutečně zajímají, a to jen na dobu nezbytně nutnou.

Záznam Dial

Záznam o vytáčení, zavěšování a době připojení vytáčených linek.

Jak číst záznam Dial*?*

```
[02/Apr/2003 15:09:27] Line "Pripojeni" dialing,
console 192.168.32.64 - standa
[02/Apr/2003 15:15:54] Line "Pripojeni" disconnected
```

- `[02/Apr/2003 15:09:27]` — datum a čas, kdy byl záznam zapsán
- `Line "Pripojeni" dialing` — začátek vytáčení linky (v uvozovkách jméno rozhraní — viz kapitola 4.1)
- `console 192.168.32.64 - standa` — způsob, jakým byla linka vytočena (z *Kerio Administration Console*, přes WWW rozhraní nebo na základě paketu z lokální sítě do Internetu). V tomto případě vytočil linku uživatel `standa` v *Kerio Administration Console*.
- `Line "Pripojeni" disconnected` — zavěšení linky

Záznam Error

Záznam *Error* zobrazuje závažné chyby, které mají zpravidla vliv na chod celého firewallu. Správce *WinRoute* by měl tento záznam pravidelně sledovat a zjištěné chyby

v co nejkratší možné době napravit. V opačném případě hrozí nejen nebezpečí, že uživatelé nebudou moci využívat některé (či dokonce všechny) služby, ale může také dojít k bezpečnostním problémům.

Typickým chybovým hlášením v záznamu *Error* bývá například: problém se spuštěním některé služby (většinou z důvodu kolize na příslušném portu), problém se zápisem na disk, s inicializací antivirové kontroly apod.

Záznam Filter

Záznam o WWW stránkách a objektech blokovaných HTTP a FTP filtrem (viz kapitoly 6.1 a 6.5) a o paketech blokovaných komunikačními pravidly (je-li v pravidle nastaveno, aby se prováděl záznam odpovídajících paketů — detaily viz kapitola 5). Každý řádek tohoto záznamu obsahuje:

- jedná-li se o pravidlo pro HTTP nebo FTP: název pravidla, uživatel a IP adresa počítače, který požadavek vyslal, přesné URL objektu
- jedná-li se o komunikační pravidlo: detailní informace o zachyceném paketu (zdrojová a cílová adresa, porty, velikost atd.)

Příklad záznamu pro komunikační pravidlo:

```
[16/Apr/2003 10:51:00] PERMIT packet to LAN,
 proto:TCP, len:47, ip/port:195.39.55.4:41272 ->
 192.168.1.11:3663, flags: ACK PSH , seq:1099972190
 ack:3795090926, win:64036, tcplen:7
```

- `[16/Apr/2003 10:51:00]` — datum a čas, kdy byl záznam zapsán
- `PERMIT packet` — akce, která byla s paketem provedena (`PERMIT` = povolen, `DENY` = zakázán, `DROP` = zahozen)
- `to LAN` — jméno rozhraní, na které byl paket směrován
- `proto:` — komunikační protokol (TCP, UDP apod.)
- `len:` — velikost paketu (včetně hlavičky) v bytech
- `ip/port:` — zdrojová IP adresa, zdrojový port, cílová IP adresa a cílový port
- `flags:` — TCP příznaky

- `seq:` — sekvenční číslo paketu
- `ack:` — sekvenční číslo potvrzení
- `win:` — velikost tzv. okénka (slouží pro řízení toku dat)
- `tcplen:` — velikost datové části paketu (bez hlavičky) v bytech

Příklad záznamu pro HTTP pravidlo:

```
[18/Apr/2003 13:39:45] ALLOW URL 'McAfee update'
 192.168.64.142 standa HTTP GET
 http://update.kerio.com/nai-antivirus/datfiles/4.x/dat-4258.zip
```

- `[18/Apr/2003 13:39:45]` — datum a čas, kdy byl záznam zapsán
- `ALLOW` — provedená akce (`ALLOW` = přístup povolen, `DENY` = přístup zakázán)
- `URL` — typ pravidla (pro URL nebo pro FTP)
- `'McAfee update'` — název pravidla
- `192.168.64.142` — IP adresa klientského počítače
- `standa` — jméno uživatele ověřeného na firewallu (není-li z daného počítače přihlášen žádný uživatel, jméno se nevypisuje)
- `HTTP GET` — použitá metoda protokolu HTTP
- `http:// ...` — požadované URL

Záznam HTTP

Kompletní záznam HTTP požadavků, které byly zpracovány inspekčním modulem protokolu HTTP (viz kapitola 8.3) nebo vestavěným proxy serverem (viz kapitola 4.4). Tento záznam má standardní formát logu proxy serveru a je vhodný ke zpracování externími analytickými nástroji. Pro správce *WinRoute* bude pravděpodobně přehlednější záznam *Web* (viz dále).

Poznámka: Do tohoto záznamu se ukládají pouze přístupy na povolené stránky. Požadavky blokované HTTP pravidly lze sledovat v záznamu *Filter* (viz výše), je-li v příslušném pravidle zapnuta volba *Zaznamenat* (viz kapitola 6.1).

Jak číst záznam HTTP?

```
[18/Apr/2003 15:07:17] 192.168.64.64 - rgabriel
 [18/Apr/2003:15:07:17 +0200]
 "GET http://www.kerio.cz/ HTTP/1.1" 304 0
```

- `[18/Apr/2003 15:07:17]` — datum a čas, kdy byl záznam zapsán
- `192.168.64.64` — IP adresa klientského počítače
- `rgabriel` — jméno uživatele ověřeného na firewallu (není-li z klientského počítače přihlášen žádný uživatel, zobrazuje se zde pomlčka)
- `[18/Apr/2003:15:07:17 +0200]` — datum a čas HTTP požadavku. Údaj `+0200` znamená časový posun vůči UTC (v tomto případě +2 hodiny — středoevropský letní čas).
- `GET` — použitá metoda protokolu HTTP
- `http://www.kerio.cz/` — požadované URL
- `HTTP/1.1` — verze protokolu HTTP
- `304` — návratový kód protokolu HTTP
- `0` — velikost přenášeného objektu (souboru) v bytech

Záznam Security

Informace, které souvisejí s bezpečností *WinRoute*. Jedná se např. o nalezené viry či neplatné IP adresy (záznam funkce *Anti-Spoofing* — viz kapitola 10.4) apod.

Příklad záznamů v okně *Security*:

```
[31/Mar/2003 09:16:11] !!! VIRUS ALERT : EICAR test file !!!
 (192.168.1.100 - admin:
 HTTP GET http://www.eicar.org/download/eicar_com.zip)
[31/Mar/2003 13:22:15] Unlock rule "Nabidka zamestnani"
 by user standa (192.168.1.200) for 60 minute(s)
```

- První záznam obsahuje informaci o nalezeném viru v HTTP komunikaci. Je zde uvedeno jméno viru, IP adresa klienta, jméno přihlášeného uživatele (není-li žádný uži-

vatel přihlášen, pak je jméno nahrazeno pomlčkou), HTTP metoda a kompletní URL požadavku.

- Druhý záznam informuje o odemknutí HTTP pravidla uživatelem. Řádek záznamu obsahuje jméno pravidla, jméno uživatele (odemykat pravidla smějí pouze přihlášení uživatelé), IP adresu klienta a dobu, na kterou je pravidlo odemčeno.

Záznam Warning

Záznam *Warning* zobrazuje varovná hlášení, což jsou ve své podstatě chyby, které nemají závažný charakter. Typickým příkladem takového varování je zpráva o chybném přihlášení uživatele (neplatné jméno a/nebo heslo), chyba při komunikaci prohlížeče s WWW administračním rozhraním apod.

Události, které způsobují varovná hlášení v tomto záznamu, nemají zásadní vliv na činnost *WinRoute*, mohou však signalizovat určité (případně potencionální) problémy, např. u konkrétních uživatelů. Záznam *Warning* může pomoci např. v případě, jestliže si jeden uživatel stěžuje na nefunkčnost některých služeb.

Příklad záznamů v okně Warning*:*

```
[15/Apr/2003 15:00:51] code 100: Kerberos 5 auth:
 user standa@firma.cz not authenticated
[15/Apr/2003 15:00:51] code 305: : Invalid password for user admin
[16/Apr/2003 10:53:20] code 300: : User jnovak doesn't exist
```

- První záznam: informace o neúspěšném ověření uživatel `standa` systémem *Kerberos* v doméně `firma.cz`
- Druhý záznam: Pokus o přihlášení uživatele `admin` s nesprávným heslem
- Třetí záznam: Pokus o přihlášení neexistujícího uživatele `jnovak`

Záznam Web

Tento záznam zobrazuje HTTP požadavky zpracované inspekčním modulem protokolu HTTP (viz kapitola 8.3) nebo vestavěným proxy serverem (viz kapitola 4.4). Narozdíl od záznamu *HTTP* jsou zde zaznamenávány pouze požadavky na stránky s textem, požadavky na objekty v rámci těchto stránek se již nezaznamenávají. URL každé stránky je pro větší přehlednost doplněno jejím názvem.

Záznam *Web* je pro správce serveru snadno čitelný a dává dobrý přehled o tom, které WWW stránky uživatelé navštívili.

Jak číst záznam Web*?*

```
[24/Apr/2003 10:29:51] 192.168.44.128 standa
 "Kerio Technologies | No Pasarán!" http://www.kerio.cz/
```

- `[24/Apr/2003 10:29:51]` — datum a čas, kdy byl záznam zapsán
- `192.168.44.128` — IP adresa klientského počítače
- `standa` — jméno přihlášeného uživatele (není-li z klientského počítače přihlášen žádný uživatel, je jméno nahrazeno pomlčkou)
- `"Kerio Technologies | No Pasarán!"` — titulek stránky

  (obsah HTML tagu `<title>`)

  Poznámka: Nelze-li titulek stránky zjistit (např. z důvodu, že je její obsah komprimován), zobrazí se zde `"Encoded content"`
- `http://www.kerio.cz/` — URL stránky

Kapitola 13

Technická podpora

Společnost *Kerio Technologies* poskytuje na produkt *Kerio WinRoute Firewall* bezplatnou e-mailovou a telefonickou technickou podporu. Kontakty naleznete na konci této kapitoly. Naši technici vám rádi ochotně pomohou s jakýmkoliv problémem.

Značné množství problémů lze ale vyřešit svépomocí (zpravidla i rychleji). Než se rozhodnete kontaktovat technickou podporu *Kerio Technologies*, proveďte prosím následující:

- Pokuste se najít odpověď v tomto manuálu. Jednotlivé kapitoly obsahují velmi detailní popis funkcí a nastavení jednotlivých částí *WinRoute*.
- Nenaleznete-li odpověď na vaši otázku zde, pokuste se ji najít na našich WWW stránkách v sekci *Technická podpora*.

Pokud ani jeden z výše uvedených postupů nepomohl vyřešit váš problém a rozhodli jste se kontaktovat naši technickou podporu, přečtěte si prosím nejprve pozorně následující kapitolu.

13.1 Informace pro technickou podporu

Abychom vám mohli co nejlépe a nejrychleji pomoci, potřebujeme získat maximum informací o vaší konfiguraci a řešeném problému. V e-mailu pro technickou podporu prosím uveďte:

Popis problému

Uveďte slovní popis vašeho problému. Snažte se uvést co nejvíce informací, které by mohly s problémem souviset (např. zda se chyba projevila po instalaci nové aplikace, upgrade *WinRoute* na novější verzi atd.).

Soubor s informacemi pro technickou podporu

V programu *Kerio Administration Console* je možné vygenerovat textový soubor obsahující informace o konfiguraci *WinRoute*. Postup vytvoření tohoto souboru:

- Spusťte *WinRoute Firewall Engine* a přihlašte se k němu v *Kerio Administration Console*.

- Je-li internetové připojení realizováno vytáčenou linkou, připojte se.
- V programu *Kerio Administration Console* stiskněte kombinaci kláves *Ctrl+S*.

Textový soubor bude uložen v domovském adresáři přihlášeného uživatele (např. `C:\Documents and Settings\Administrator`) pod názvem `kerio_support_info.txt`.

Poznámka: Soubor `kerio_support_info.txt` vytváří program *Kerio Administration Console*. V případě vzdálené správy bude tedy uložen na počítači, ze kterého *WinRoute* spravujete, nikoliv na počítači (serveru), kde běží *WinRoute Firewall Engine*.

Soubory se záznamy o chybách

V adresáři, kde je *WinRoute* nainstalován (typicky `C:\Program Files\Kerio\WinRoute Firewall`), je vytvořen podadresář `logs`. V něm naleznete soubory `error.log` a `warning.log`. Připojte tyto dva soubory jako přílohy k e-mailu pro technickou podporu.

13.2 Kontakty

Česká Republika

Kerio Technologies s.r.o.
Sedláčkova 16
301 11 PLZEŇ
Tel.: +420 377 338 901
E-mail: `support@kerio.cz/`
`http://www.kerio.cz/`

USA

Kerio Technologies Inc.
2041 Mission College Blvd., Suite 100
Santa Clara, CA 95054
Tel.: +1 408 496 4500
E-mail: `support@kerio.com`
`http://www.kerio.com/`

Velká Británie

Kerio Technologies UK Ltd.
Sheraton House
Castle Park
Cambridge, CB3 0AX
Tel.: +44 1223 370 136, +44 8707 442 205
E-mail: support@kerio.co.uk
http://www.kerio.co.uk/

Kapitola 14

Slovníček pojmů

DHCP DHCP (*Dynamic Host Configuration Protocol*) slouží k automatické konfiguraci počítačů v síti. IP adresy jsou přidělovány dynamicky z definovaného rozsahu. Klientskému počítači mohou být kromě IP adresy přiděleny i další parametry — např. adresa výchozí brány, adresa DNS serveru, jméno lokální domény atd.

DNS DNS (*Domain Name System*) je celosvětová distribuovaná databáze obsahující jména počítačů, odpovídající IP adresy a některé další informace. Jména jsou řazena do tzv. domén s hierarchickou strukturou.

Firewall Software nebo hardwarové zařízení, které chrání počítač nebo počítačovou síť před průnikem zvenčí (typicky z Internetu).

Pro účely tohoto manuálu je výrazem *firewall* označován počítač, na kterém běží *WinRoute*.

IP adresa 32-bitové číslo jednoznačně určující počítač v Internetu. Zapisuje v desítkové soustavě jako čtveřice bytů (`0–255`) oddělených tečkami (např. `195.129.33.1`). Každý paket obsahuje informaci, odkud byl vyslán (zdrojová IP adresa) a kam má být doručen (cílová IP adresa).

Kerberos Systém pro bezpečné ověřování uživatelů v síťovém prostředí. Byl vyvinut na univerzitě MIT a je standardně používán pro ověřování uživatelů v prostředí Windows 2000. Uživatelé se přihlašují svým heslem k centrálnímu serveru (KDC, Key Distribution Center, Windows 2000 domain controller) a od něho dostávají šifrované vstupenky (tickets) pro přihlášení k serverům v síti.

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:

- překlad zdrojových adres (*Source NAT, SNAT*) — v paketech jdoucích z lokální sítě do Internetu se zdrojová (privátní) IP adresa nahrazuje vnější (veřejnou) adre-

sou firewallu. O každé komunikaci zahájené z lokální sítě se provádí záznam do tzv. NAT tabulky. Jestliže příchozí paket z Internetu odpovídá některému z těchto záznamů, jeho cílová IP adresa je nahrazena adresou příslušného počítače v lokální síti a paket je směrován na tento počítač. Pokud příchozí paket nevyhovuje žádnému záznamu v NAT tabulce, je zahozen.

- překlad cílových adres (*Destination NAT, DNAT*, též mapování portů) — slouží ke zpřístupnění služeb v lokální síti z Internetu. Jestliže příchozí paket z Internetu vyhoví určitým podmínkám, jeho cílová IP adresa je nahrazena adresou počítače v lokální síti, kde příslušná služba běží, a paket je směrován na tento počítač.

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 Základní datová jednotka přenášená počítačovou sítí. Každý paket se skládá z tzv. hlavičky, která obsahuje řídicí informace (tj. např. zdrojovou a cílovou adresu, typ protokolu apod.), a datové části obsahující vlastní přenášená data. Data přenášená sítí jsou vždy rozdělena do (relativně malých) paketů. Při chybě v jednom paketu či ztrátě paketu nemusí být opakován celý přenos, stačí zopakovat vyslání chybného paketu.

Port 16-bitové číslo (`1–65535`) používané protokoly TCP a UDP pro identifikaci aplikací (služeb) na daném počítači. Na jednom počítači (jedné IP adrese) může běžet více aplikací současně (např. WWW server, poštovní klient, WWW klient — prohlížeč, FTP klient atd.). Každá aplikace je však jednoznačně určena číslem portu. Porty `1–1023` jsou vyhrazené a používají je standardní, příp. systémové služby (např. `80` = WWW). Porty nad `1024` (včetně) mohou být volně použity libovolnou aplikací (typicky klientem jako zdrojový port nebo nestandardní aplikací serverového typu).

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.

Síťové rozhraní 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.

Směrovací tabulka Množina pravidel pro posílání paketů mezi jednotlivými rozhraními daného systému. Směrování se provádí podle cílové IP adresy paketu. V operačních systémech Windows lze směrovací tabulku zobrazit příkazem `route print`.

SSL Protokol *Secure Socket Layer* slouží k zabezpečení a šifrování TCP spojení. Původně byl navržen firmou Netscape pro zabezpečení přenosu WWW stránek protokolem HTTP, dnes je využíván téměř všemi standardními internetovými protokoly — SMTP, POP3, IMAP, LDAP atd.

Na začátku komunikace se nejprve asymetrickou šifrou provede výměna šifrovacího klíče, který je pak použit pro (symetrické) šifrování vlastních dat.

TCP *Transmission Control Protocol* je protokol transportní úrovně, který zaručuje spolehlivé a sekvenční doručení dat. Vytváří tzv. virtuální spojení a má prostředky k opravě chyb a řízení toku dat. Je využíván většinou aplikačních protokolů, které vyžadují spolehlivé přenesení všech dat (např. *HTTP*, *FTP*, *SMTP*, *IMAP* atd.).

Protokol *TCP* používá speciální řídicí informace — tzv. příznaky (*flags*):

- *SYN* (Synchronize) — navázání spojení (první paket v každém spojení)
- *ACK* (Acknowledgement) — potvrzení přijatých dat
- *RST* (Reset) — požadavek ukončení spojení a navázání nového
- *URG* (Urgent) — urgetní paket
- *PSH* (Push) — požadavek okamžitého předání dat vyšším vrstvám TCP/IP
- *FIN* (Finalize) — ukončení spojení

TCP/IP Společné označení pro komunikační protokoly používané v Internetu (např. *IP*, *ICMP*, *TCP*, *UDP* atd.). *TCP/IP* není konkrétní protokol!

TLS Protokol *Transport Layer Security* je nástupcem SSL, de facto SSL verze 3.1. Tato verze je standardizována organizací IETF a přijata všemi významnými firmami (např. Microsoft Corporation).

UDP *User Datagram Protokol* je protokol transportní úrovně, který přenáší data v jednotlivých zprávách (tzv. datagramech). Nevytváří spojení, nezaručuje spolehlivé a sekvenční doručení dat a neumožňuje řízení toku dat a opravu chyb. Je vhodný pro přenos malého objemu dat (např. DNS dotazy) nebo v případech, kdy je rychlost důležitější než spolehlivost (např. přenos zvuku a videa v reálném čase).

VPN Virtuální privátní síť (*Virtual Private Network, VPN*) představuje bezpečné propojení privátních sítí (např. jednotlivých poboček firmy) přes Internet. Spojení mezi

oběma sítěmi (tzv. tunel) je šifrováno, což zabraňuje odposlechu přenášených dat. Pro vytváření VPN existují speciální protokoly, mezi nejrozšířenější patří standard *IPSec* a *PPTP* (*Point-to-Point Tunnelling Protocol*) firmy *Microsoft*.

Kapitola 15

Rejstřík