Kerio WinRoute Firewall 6

Příručka administrátora

Kerio Technologies s.r.o.

Tento manuál popisuje konfiguraci a správu produktu *Kerio WinRoute Firewall* ve verzi *6.7.1*. Změny vyhrazeny. Uživatelská rozhraní *Kerio StaR* a *Kerio Clientless SSL-VPN* jsou popsána v samostatném manuálu *Kerio WinRoute Firewall — Příručka uživatele*. Aplikace *Kerio VPN Client* je popsána v samostatném manuálu *Kerio VPN Client — Příručka uživatele*.

Aktuální verzi produktu naleznete na WWW stránce http://www.kerio.cz/cz/firewall/download, další dokumentaci na stránce http://www.kerio.cz/cz/firewall/manual.

Produkty *Kerio WinRoute Firewall* a *Kerio VPN Client* obsahují software volně šiřitelný ve formě zdrojových kódů (open source). Seznam tohoto software je uveden v příloze B.

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 síťová rozhraní — jedno připojené do lokální sítě (např. síťový adaptér *Ethernet* nebo *WiFi*) a jedno připojené k Internetu (např. síťový adaptér *Ethernet* nebo *WiFi*, USB ADSL modem, analogový modem nebo ISDN adaptér).

   V operačním systému *Windows* 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* a v průvodci zadejte potřebné základní parametry (podrobnosti viz kapitola 2.4, resp. 2.7).

3. Nastavte skupiny rozhraní a základní komunikační pravidla pomocí *Průvodce komunikačními pravidly* (viz kapitola 7.1).

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 8.2.

5. Zkontrolujte nastavení modulu *DNS*. Chcete-li prohledávat soubor `hosts` a/nebo tabulky DHCP serveru, nezapomeňte uvést lokální DNS doménu. Podrobnosti viz kapitola 8.1.

6. Nastavte mapování uživatelů z *Active Directory* domény, případně vytvořte nebo importujte lokální uživatelské účty a skupiny. Nastavte uživatelům požadovaná přístupová práva. Podrobnosti viz kapitola 15.

7. Definujte skupiny IP adres (kapitola 14.1), časové intervaly (kapitola 14.2) a skupiny URL (kapitola 14.4), které použijete při definici pravidel (viz kapitola 14.2).

8. Vytvořte pravidla pro URL (kapitola 12.2) a nastavte modul *Kerio Web Filter* (kapitola 12.3). Nastavte HTTP cache a automatickou konfiguraci prohlížečů (kapitola 8.5). Definujte pravidla pro FTP (kapitola 12.5).

9. Vyberte antivirový program a nastavte typy objektů, které mají být kontrolovány.

   Při použití integrovaného antiviru *McAfee* zkontrolujte a případně upravte nastavení automatické aktualizace.

   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* (*Internet Explorer*) nebo zadejte URL pro automatickou konfiguraci (jiné typy prohlížečů). Podrobnosti naleznete v kapitole 8.5.

    - *Ruční konfigurace* — zvolte připojení lokální sítí, případně nastavte IP adresu a port proxy serveru (viz kapitola 8.4).

Kapitola 2

Úvod

2.1 Novinky ve verzi 6.7.1

WinRoute ve verzi 6.7.1 nabízí tyto nové funkce:

Kerio WinRoute Firewall Software Appliance / VMware Virtual Appliance

Kerio WinRoute Firewall je nyní k dispozici ve formě tzv. softwarového zařízení (*Software Appliance / VMware Virtual Appliance*). Toto zařízení je distribuováno jako kompletní instalační balík firewallu včetně operačního systému a je určeno pro instalaci na fyzický nebo virtuální počítač bez operačního systému. *Software Appliance* není možné nainstalovat na počítač současně s jiným operačním systémem. Instalační balík samostatného produktu pro instalaci na stávající systém *Linux* není k dispozici.

Kerio WinRoute Firewall v edici *Software Appliance / VMware Virtual Appliance* nabízí stejné funkce jako edice pro *Windows*, s výjimkou rozhraní *Kerio Clientless SSL-VPN*.

Webové rozhraní pro správu (Web Administration)

Nové rozhraní *Web Administration* umožňuje vzdálenou i lokální správu firewallu bez nutnosti instalace programu *Kerio Administration Console*. Toto rozhraní umožňuje konfiguraci nejdůležitějších parametrů *WinRoute* — rozhraní, komunikačních pravidel, pravidel pro filtrování protokolů *HTTP* a *FTP*, uživatelských účtů a skupin atd. Program *Kerio Administration Console* je i nadále k dispozici a umožňuje nastavení všech konfiguračních voleb.

Rozhraní *Web Administration* je dostupné na adrese `https://server:4081/admin` (`server` má význam jména nebo IP adresy firewallu a `4081` je výchozí port jeho WWW rozhraní).

Více v kapitole 3.

Export a import konfigurace

WinRoute nyní obsahuje nástroj pro zálohování a obnovení kompletní konfigurace, včetně lokálních uživatelských účtů a SSL certifikátů. Tyto funkce umožňují snadné a rychlé obnovení firewallu v případě selhání hardware, přenos na jiný počítač nebo klonování identické konfigurace na více firewallů. Export a import konfigurace lze provést v rozhraní *Web Administration*.

Více v kapitole 25.1.

Nový modul pro hodnocení obsahu WWW stránek Kerio Web Filter

Kerio Web Filter slouží k filtrování WWW stránek podle kategorií jejich obsahu. Ve *WinRoute* nahrazuje modul *ISS OrangeWeb Filter*. Způsob vytváření filtrovacích pravidel zůstává stejný.

Více v kapitole 12.3.

Podpora Windows 7

Kerio WinRoute Firewall nyní plně podporuje nový operační systém *Microsoft Windows 7*.

2.2 Konfliktní software

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.

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*.

Kolize nízkoúrovňových ovladačů

WinRoute vykazuje kolize se systémovými službami a aplikacemi, jejichž nízkoúrovňové ovladače používají stejnou nebo podobnou technologii. Jedná se zejména o tyto typy služeb a aplikací:

- Systémová služba *Windows Firewall / Sdílení připojení k Internetu*. Tuto službu dokáže *WinRoute* detekovat a automaticky vypnout.
- Systémová služba *Směrování a vzdálený přístup (RRAS)* v operačních systémech typu *Windows Server*. Tato služba rovněž umožňuje sdílení internetového připojení (NAT). *WinRoute* dokáže detekovat, zda je NAT ve službě *RRAS* aktivní, a pokud ano, zobrazí varování. Správce serveru pak musí NAT v konfiguraci služby *RRAS* vypnout.
  Pokud není aktivní NAT, nedochází ke kolizím a *WinRoute* může být používán společně se službou *RRAS*.
- Síťové firewally — např. *Microsoft ISA Server*.
- Osobní firewally — např. *Sunbelt Personal Firewall*, *Zone Alarm*, *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.
  Pokud to okolnosti dovolují, doporučujeme využít VPN řešení obsažené ve *WinRoute* (podrobnosti viz kapitola 23). V opačném případě doporučujeme otestovat konkrétní VPN server či VPN klienta se zkušební verzí *WinRoute* a případně kontaktovat technickou podporu firmy *Kerio Technologies* (viz kapitola 26).
  Poznámka: Implementace VPN obsažená v operačním systému *Windows* (založená na protokolu PPTP) 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, které *WinRoute* nabízí, pak *WinRoute* využívá tyto porty:

- `53/UDP` — modul *DNS*,
- `67/UDP` — *DHCP server*,

- `1900/UDP` — služba *SSDP Discovery*,
- `2869/TCP` — služba *UPnP Host*.
  Služby *SSDP Discovery* a *UPnP Host* jsou součásti podpory protokolu UPnP (viz kapitola 18.2).
- `44333/TCP+UDP` — komunikace mezi programem *Kerio Administration Console* a *WinRoute Firewall Engine*. Tuto službu jako jedinou nelze vypnout.

Následující služby používají uvedené porty ve výchozí konfiguraci. Porty těchto služeb lze změnit.

- `443/TCP` — server rozhraní *SSL-VPN* (pouze ve *WinRoute* na systému *Windows* — viz kapitola 24),
- `3128/TCP` — HTTP proxy server (viz kapitola 8.4),
- `4080/TCP` — WWW rozhraní firewallu (viz kapitola 11),
- `4081/TCP` — zabezpečená (SSL) verze WWW rozhraní firewallu (viz kapitola 11),
- `4090/TCP+UDP` — proprietární VPN server (podrobnosti viz kapitola 23).

Antivirové programy

Řada moderních desktopových antivirů (tj. antivirů určených pro ochranu pracovních stanic) provádí také antivirovou kontrolu síťové komunikace — typicky *HTTP*, *FTP* a e-mailových protokolů. *WinRoute* rovněž poskytuje tuto funkci, a proto zde dochází ke kolizím. Z tohoto důvodu doporučujeme na počítač s *WinRoute* instalovat vždy serverovou verzi zvoleného antivirového programu. Serverovou verzi antiviru lze zároveň využít pro kontrolu síťové komunikace ve *WinRoute*, případně jako doplňkovou kontrolu k integrovanému antivirovému modulu *McAfee* (podrobnosti viz kapitola 13).

Má-li antivirový program tzv. rezidentní štít (automatická kontrola všech čtených a zapisovaných souborů), pak je třeba z kontroly vyloučit podadresáře `cache` (HTTP cache *WinRoute* — viz kapitola 8.5) a `tmp` (používá se pro antivirovou kontrolu). Pokud *WinRoute* využívá antivirový program pro kontrolu objektů stahovaných protokoly HTTP a FTP (viz kapitola 13.3), pak vyloučení adresáře cache z kontroly souborů na disku nepředstavuje žádnou hrozbu — soubory uložené v tomto adresáři jsou již antivirovým programem zkontrolovány.

Integrovaný antivirový modul *McAfee* nevykazuje žádnou interakci s antivirovým programem nainstalovaným na počítači s *WinRoute* (za předpokladu, že jsou splněny výše uvedené podmínky).

2.3 Systémové požadavky

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

- CPU 1 GHz,
- 1 GB operační paměti RAM,
- Dvě síťová rozhraní (včetně vytáčených).

Pro operační systém *Windows*:

- 50 MB diskového prostoru pro instalaci produktu *Kerio WinRoute Firewall*.

- Diskový prostor pro statistiky (viz kapitola 21) a záznamy (dle intenzity provozu a zvolené úrovně logování — viz kapitola 22).
- Z důvodu bezpečnosti nainstalovaného produktu (zejména jeho konfiguračních souborů) doporučujeme použít souborový systém *NTFS*.

Pro *Kerio WinRoute Firewall Software Appliance*:

- Pevný disk o kapacitě minimálně 3 GB.
- Na počítači nemusí být nainstalován žádný operační systém. Existující OS bude při instalaci vymazán.

Pro *Kerio WinRoute Firewall VMware Virtual Appliance*:

- *VMware Player*, *VMware Workstation* nebo *VMware Server*.
- 3 GB diskového prostoru.

Pro přístup k webovým službám *WinRoute* (*Kerio StaR* — viz kapitola 21 a *Kerio SSL-VPN* — viz kapitola 24) je možné použít tyto WWW prohlížeče:

- *Internet Explorer 7 a vyšší*,
- *Firefox 2 a vyšší*,
- *Safari 3 a vyšší*.

2.4 Instalace - Windows

Instalační balíky

Kerio WinRoute Firewall je distribuován ve dvou edicích: pro 32-bitové platformy a pro 64-bitové platformy (viz stránka pro stažení produktu: http://www.kerio.cz/cz/firewall/download).

32-bitovou edici (instalační balík označený „*win32*“) lze nainstalovat na tyto operační systémy:

- *Windows 2000*,
- *Windows XP* (32 bit),
- *Windows Server 2003* (32 bit),
- *Windows Vista* (32 bit),
- *Windows Server 2008* (32 bit).

64-bitovou edici (instalační balík označený „*win64*“) lze nainstalovat na tyto operační systémy:

- *Windows XP* (64 bit),
- *Windows Server 2003* (64 bit),
- *Windows Vista* (64 bit),
- *Windows Server 2008* (64 bit).

Starší verze operačních systémů *Windows* nejsou podporovány.

Poznámka:

1. Instalační balíky *WinRoute* již obsahují administrační program *Kerio Administration Console*. Samostatný instalační balík *Kerio Administration Console* (soubor

`kerio-kwf-admin*.exe`) je určen pro instalaci na jiný počítač za účelem plné vzdálené správy. Tento balík je společný pro 32-bitové i 64-bitové verze systému *Windows*. Podrobnosti o správě *WinRoute* viz kapitola 3.

2. Pro správnou funkci rozhraní *Kerio StaR* (viz kapitola 21) musí operační systém počítače s *WinRoute* podporovat všechny jazyky, které budou v rozhraní *Kerio StaR* používány. Pro některé jazyky (např. japonština a čínština) může být vyžadována instalace podpůrných souborů. Bližší informace naleznete v dokumentaci k příslušnému operačnímu systému.

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 k lokální síti (Ethernet, WiFi apod.) a rozhraní připojené k Internetu. Internetovým rozhraním může být buď síťový adaptér (Ethernet, WiFi 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 k lokální síti, tak k Internetu (vhodným nástrojem je např. příkaz `ping`, který zjišťuje dobu odezvy počítače zadaného jménem nebo IP adresou).

Provedení těchto kroků vám ušetří mnoho komplikací při pozdějším odstraňování případných problémů.

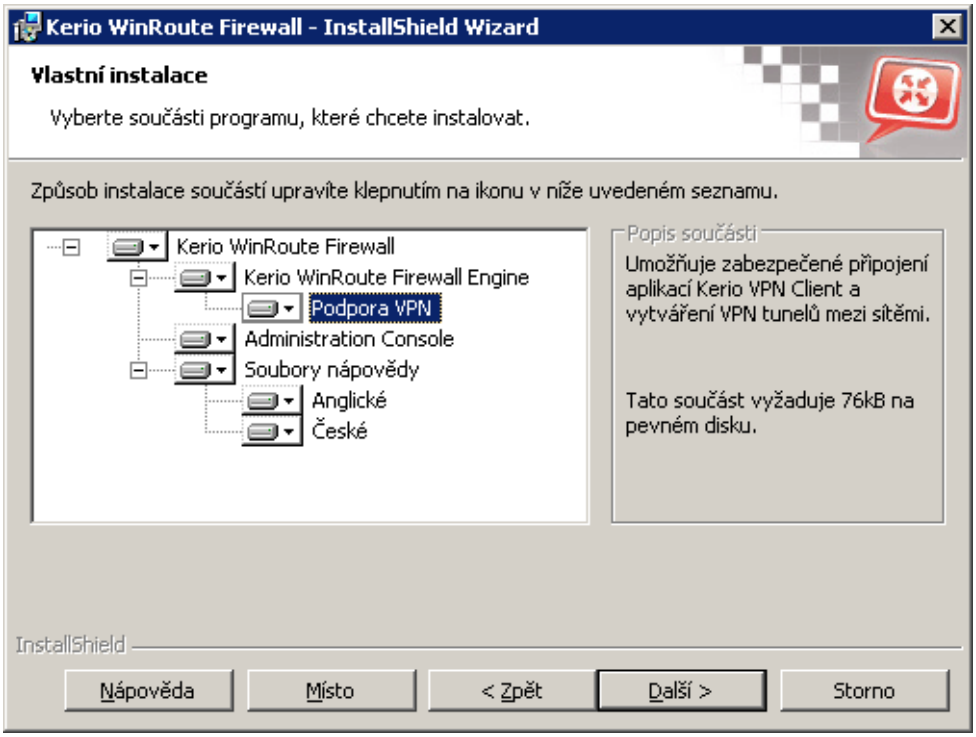
Poznámka: Všechny podporované operační systémy obsahují ve standardní instalaci všechny komponenty, které *WinRoute* pro svoji činnost vyžaduje.

Postup instalace a počáteční konfigurace

Po spuštění instalačního programu (např. `kerio-kwf-6.6.0-5700-win32.exe`) lze vybrat jazyk instalačního programu. Výběr jazyka ovlivňuje pouze samotnou instalaci, jazyk uživatelského rozhraní lze pak nastavit nezávisle pro jednotlivé komponenty *WinRoute*.

V instalačním programu je možné zvolit typ instalace — *Úplnou* nebo *Vlastní*. Vlastní instalace umožňuje výběr volitelných komponent programu:

- *Kerio WinRoute Firewall Engine* — vlastní výkonné jádro aplikace.
- *Podpora VPN* — proprietární VPN řešení firmy *Kerio Technologies* (*Kerio VPN*).
- *Administration Console* — program *Kerio Administration Console* (univerzální konzole pro správu serverových aplikací firmy *Kerio Technologies*) s modulem pro správu *WinRoute*.
- *Soubory nápovědy* — soubory nápovědy (tato příručka ve formátu *HTML Help*). Podrobnosti o souborech nápovědy viz samostatný manuál *Kerio*



Obrázek 2.1 Instalace — výběr volitelných komponent

Administration Console — Nápověda (k dispozici na WWW stránce http://www.kerio.cz/cz/firewall/manual).

Podrobný popis komponent *WinRoute* naleznete v kapitole 2.9. Proprietární VPN řešení je detailně popsáno v kapitole 23.

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 2.5).

Za normálních okolností není třeba po instalaci počítač restartovat (restart může být vyžadován, pokud instalační program přepisuje sdílené soubory, které jsou právě používány). Po dokončení instalace se automaticky spustí *WinRoute Firewall Engine*, tj. vlastní výkonné jádro programu (běží jako systémová služba) a také *WinRoute Engine Monitor*.

Poznámka:

1. Je-li zvolen typ instalace *Vlastní*, pak se instalační program chová takto:
   - všechny označené komponenty se nainstalují nebo aktualizují,
   - všechny neoznačené komponenty se nenainstalují nebo odstraní.

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

2. Instalační program neumožňuje nainstalovat samostatnou komponentu *Administration Console*. Pro instalaci *Administration Console* za účelem plné vzdálené správy je určen samostatný instalační balík (soubor `kerio-kwf-admin*.exe`).

Ochrana nainstalovaného produktu

Pro zajištění plné bezpečnosti firewallu je důležité, aby neoprávněné osoby neměly žádný přístup k souborům aplikace (zejména ke konfiguračním souborům). Je-li použit souborový systém *NTFS*, pak *WinRoute* při každém svém startu obnovuje nastavení přístupových práv k adresáři, ve kterém je nainstalován (včetně všech podadresářů): pouze členům skupiny *Administrators* a lokálnímu systémovému účtu (*SYSTEM*) je povolen přístup pro čtení i zápis, ostatní uživatelé nemají žádný přístup.

Upozornění

Při použití souborového systému *FAT32* nelze soubory *WinRoute* výše popsaným způsobem zabezpečit. Z tohoto důvodu doporučujeme instalovat *WinRoute* výhradně na disk se souborovým systémem *NTFS*.

Kolizní programy a systémové služby

Instalační program *WinRoute* detekuje programy a systémové služby, které by mohly způsobovat kolize se službou *WinRoute Firewall Engine*.

1. Systémové komponenty *Windows Firewall*[1] a *Sdílení připojení k Internetu*

   Tyto komponenty zajišťují podobné nízkoúrovňové funkce jako *WinRoute*. Pokud by byly spuštěny společně s *WinRoute*, nefungovala by síťová komunikace správně a *WinRoute* by mohl být nestabilní. Obě tyto komponenty jsou realizovány systémovou službou *Windows Firewall / Sdílení připojení k Internetu* (*Windows Firewall / Internet Connection Sharing*)[2].

   Upozornění

   Pro správnou funkci *WinRoute musí* být služba *Windows Firewall / Sdílení připojení k Internetu* zastavena a zakázána!

2. *Hostitel zařízení UPnP* (*Universal Plug and Play Device Host*) a *Služba rozpoznávání pomocí protokolu SSDP* (*SSDP Discovery Service*)

   Uvedené služby tvoří podporu protokolu *UPnP* (Universal Plug and Play) v operačních systémech *Windows XP*, *Windows Server 2003*, *Windows Vista* a *Windows Server 2008*. Tyto služby však vykazují kolize s podporou protokolu *UPnP* ve *WinRoute* (viz kapitola 18.2).

Instalační program *WinRoute* při instalaci zobrazí dialog, ve kterém může uživatel zakázat konfliktní systémové služby.

[1] V operačním systému *Windows XP Service Pack 1* a starších verzích má integrovaný firewall název *Brána Firewall připojení k Internetu* (*Internet Connection Firewall*).

[2] V uvedených starších verzích operačního systému *Windows* má služba název *Součást ICF (Brána Firewall připojení k Internetu) / součást ICS (Sdílení připojení k Internetu)*; v angličtině *Internet Connection Firewall / Internet Connection Sharing*.

Obrázek 2.2 Zakázání konfliktních systémových služeb při instalaci

Ve výchozím nastavení instalační program *WinRoute* zakáže všechny výše uvedené kolizní služby. Za normálních okolností není třeba toto nastavení měnit. Obecně existují následující možnosti:

- Služba *Windows Firewall / Internet Connection Sharing (ICS)* by měla být vždy zakázána. Pokud bude tato služba spuštěna, nebude *WinRoute* fungovat správně. Uvedenou volbu při instalaci lze chápat spíše jako varování, že tato služba je spuštěna a musí být zastavena a zakázána.
- Pokud chceme využít podporu protokolu *UPnP* ve *WinRoute* (viz kapitola 18.2), pak je nutné zakázat také služby *Hostitel zařízení UPnP* (*Universal Plug and Play Device Host*) a *Služba rozpoznávání pomocí protokolu SSDP* (*SSDP Discovery Service*).
- Nechceme-li využívat podporu *UPnP* ve *WinRoute*, není nutné služby *Hostitel zařízení UPnP* (*Universal Plug and Play Device Host*) a *Služba rozpoznávání pomocí protokolu SSDP* (*SSDP Discovery Service*) zakazovat.

Poznámka:

1. *WinRoute* při každém svém startu automaticky detekuje, zda je spuštěna systémová služba *Windows Firewall / Sdílení připojení k Internetu* (*Windows Firewall / Internet Connection Sharing*), a pokud ano, automaticky ji zastaví a zapíše informaci do záznamu *warning*. Tím je ošetřen případ, že dojde k povolení/spuštění této služby v době, kdy je již *WinRoute* nainstalován.

2. V operačních systémech *Windows XP Service Pack 2*, *Windows Server 2003*, *Windows Vista* a *Windows Server 2008* se *WinRoute* také automaticky registruje v *Centru zabezpečení*

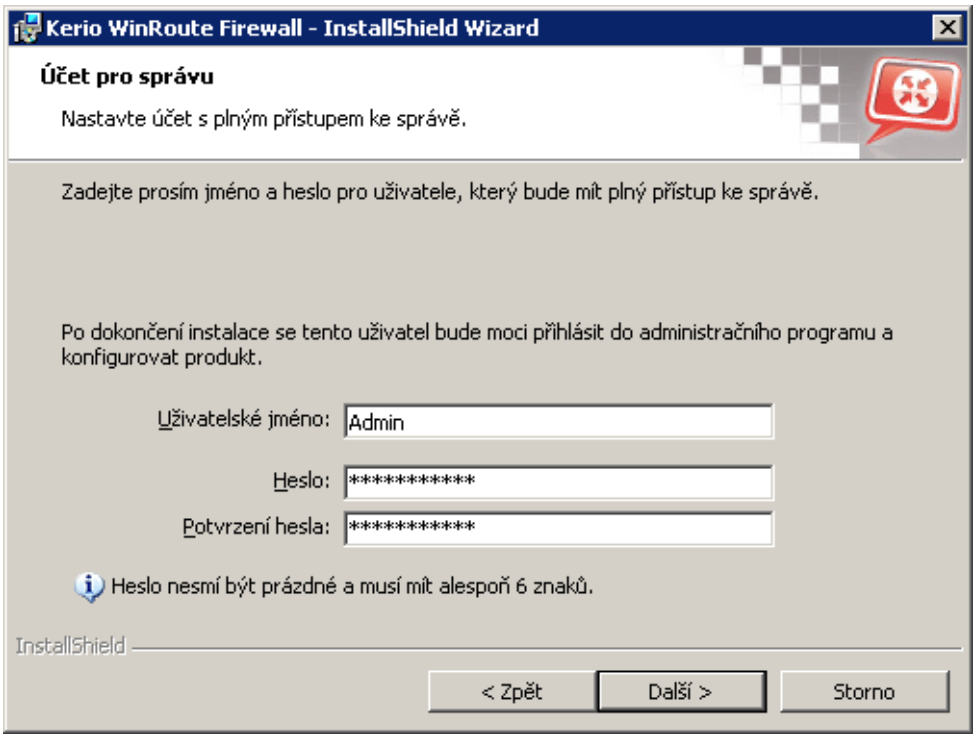
(*Security Center*). To znamená, že *Centrum zabezpečení* bude vždy správně indikovat stav firewallu a nebude zobrazováno varování, že systém není chráněn.

2.5 Průvodce počáteční konfigurací (Windows)

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

Nastavení administrátorského jména a hesla

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



Obrázek 2.3 Počáteční konfigurace — nastavení uživatelského jména a hesla pro administraci

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

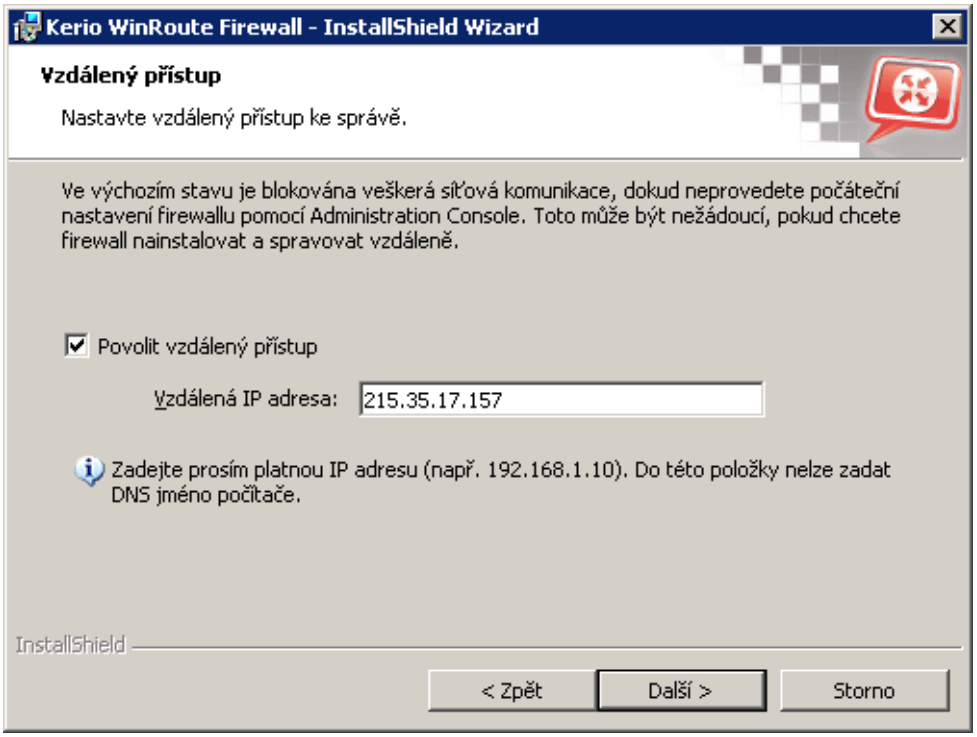
Poznámka: Pokud je instalace spuštěna jako upgrade, pak je tento krok přeskočen — administrátorský účet již existuje.

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 7). 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. *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.



Obrázek 2.4 Počáteční konfigurace — povolení vzdálené správy

Povolit vzdálený přístup
: Tato volba povoluje plný přístup k počítači s *WinRoute* z jedné vybrané IP adresy.

Vzdálená IP adresa
: 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 7.1) se pravidlo pro povolení vzdáleného přístupu zruší.

2.6 Upgrade a deinstalace - Windows

Upgrade

Chceme-li provést upgrade (tj. instalovat novější verzi získanou např. z WWW stránek výrobce), stačí jednoduše spustit instalaci nové verze.

Před instalací je třeba zavřít všechna okna programu *Kerio Administration Console*. Komponenty *WinRoute Firewall Engine* a *WinRoute Engine Monitor* dokáže instalační program ukončit sám.

Při instalaci bude rozpoznán adresář, kde je stávající verze nainstalována, a nahrazeny příslušné soubory novými. Přitom zůstane zachována licence, veškerá nastavení i soubory záznamů.

Poznámka: Tento postup je platný pro upgrade mezi verzemi stejné řady (např. z verze *6.6.0* na verzi *6.6.1*) nebo z verze předchozí řady na verzi následující řady (např. z verze *6.5.2* na verzi *6.6.0*). Při upgrade z verze starší řady (např. *6.3.1*) není zaručena plná přenositelnost konfigurace a doporučuje se provést upgrade „skokově“ (např. *6.3.1* → *6.4.0* → *6.5.0* → *6.6.0*), případně starou verzi nejprve odinstalovat s odstraněním všech souborů a poté provést „čistou“ instalaci nové verze.

Automatická kontrola nových verzí

WinRoute umožňuje automaticky kontrolovat, zda se na serveru firmy *Kerio Technologies* nachází novější verze, než je aktuálně nainstalována. Je-li nalezena nová verze, nabídne *WinRoute* její stažení a instalaci.

Podrobné informace naleznete v kapitole 16.3.

Deinstalace

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 instalačním adresáři *WinRoute*

(typicky `C:\Program Files\Kerio\WinRoute Firewall`)

— konfigurační soubory, SSL certifikáty, licenční klíč, záznamy apod.

Obrázek 2.5 Deinstalace — dotaz na smazání souborů vytvořených za běhu WinRoute

Ponechání těchto souborů může mít význam např. pro přenos konfigurace na jiný počítač nebo v případě, kdy si nejsme jisti, zda máme zálohované SSL certifikáty vystavené důvěryhodnou certifikační autoritou.

Při deinstalaci instalační program *WinRoute* automaticky obnoví původní stav systémových služeb *Windows Firewall / Sdílení připojení k Internetu* (*Windows Firewall / Internet Connection Sharing*)[1], *Hostitel zařízení UPnP* (*Universal Plug and Play Device Host*) a *Služba rozpoznávání pomocí protokolu SSDP* (*SSDP Discovery Service*).

2.7 Instalace - Software Appliance a VMware Virtual Appliance

WinRoute v edici softwarového zařízení je distribuován:

- ve formě ISO obrazu instalačního CD, ze kterého lze zavést systém a nainstalovat firewall na fyzický nebo virtuální počítač (*Software Appliance*),
- ve formě virtuálního zařízení pro *VMware* (*VMware Virtual Appliance*).

Samostatný instalační balík *WinRoute* pro instalaci na stávající systém *Linux* není k dispozici.

Instalace *Software Appliance / VMware Virtual Appliance* probíhá v několika jednoduchých krocích:

Spuštění instalace

Software Appliance

ISO obraz instalačního CD můžeme vypálit na fyzické CD a z tohoto CD spustit instalaci systému na zvoleném cílovém počítači (fyzickém nebo virtuálním). V případě virtuálního počítače lze ISO obraz také přímo připojit jako virtuální CD mechaniku, bez nutnosti vypalování CD.

Poznámka: Kerio WinRoute Firewall Software Appliance není možné nainstalovat na počítač současně s jiným operačním systémem. Existující operační systém na cílovém disku bude při instalaci vymazán.

VMware Virtual Appliance

Distribuční balík (ve formátu *Zip*) rozbalíme a soubor s příponou `.vmx` otevřeme ve zvoleném produktu *VMware* (*VMware Player*, *VMware Workstation*, *VMware Server*). Tím se spustí instalátor produktu *Kerio WinRoute Firewall*.

Následující kroky jsou již shodné pro *Software Appliance* i *Virtual Appliance*.

Volba jazyka

Zvolený jazyk bude použit nejen pro instalaci *WinRoute*, ale také pro konzoli firewallu (viz kapitola 2.11).

Výběr cílového pevného disku

Pokud instalační program detekuje v počítači více pevných disků, pak je potřeba zvolit disk, na který má být *WinRoute* nainstalován. Obsah vybraného disku bude před vlastní instalací *WinRoute* kompletně vymazán, zatímco ostatní disky instalace nijak neovlivní.

Je-li v počítači detekován pouze jeden pevný disk, instalační program přejde ihned k následujícímu kroku. Není-li nalezen žádný pevný disk, pak bude instalace ukončena. Příčinou této chyby bývá nejčastěji nepodporovaný typ pevného disku nebo závada hardware.

Výběr síťového rozhraní pro lokální síť a přístup ke správě

Instalační program zobrazí všechna detekovaná síťová rozhraní firewallu. Z nich je nutné vybrat rozhraní, které je připojeno do lokální (důvěryhodné) sítě, ze které budeme firewall vzdáleně spravovat.

V praxi se může často stát, že má počítač více rozhraní stejného typu, a tudíž nelze jednoduše rozpoznat, které rozhraní je připojené do lokální sítě a které do Internetu. Určitým vodítkem mohou být hardwarové adresy adaptérů, případně lze postupovat experimentálně — vybereme některé rozhraní, dokončíme instalaci a zkusíme se připojit ke správě. Pokud se připojení nepodaří, změníme nastavení jednotlivých rozhraní volbou *Konfigurace sítě* v hlavní nabídce konzole firewallu (viz kapitola 2.11).

Dále může nastat situace, že instalační program nerozpozná některé nebo všechny síťové adaptéry. V takovém případě je doporučeno vyměnit fyzický adaptér za jiný typ, případně

změnit typ virtuálního adaptéru (pokud to daný virtuální počítač umožňuje) nebo nainstalovat *WinRoute Software Appliance* do jiného typu virtuálního počítače. Tento problém doporučujeme konzultovat s technickou podporou společnosti *Kerio Technologies* (viz kapitola 26).

Pokud není detekován žádný síťový adaptér, pak není možné v instalaci *WinRoute* pokračovat.

Nastavení IP adresy lokálního rozhraní

Vybranému lokálnímu rozhraní je potřeba nastavit IP adresu a masku subsítě. Tyto parametry mohou být přiděleny automaticky DHCP serverem, anebo zadány ručně.

Doporučujeme nastavit parametry lokálního rozhraní ručně, a to z následujících důvodů:

- Automaticky přidělovaná IP adresa se může měnit, což by způsobovalo problémy s připojením ke správě firewallu (IP adresu sice lze na DHCP serveru rezervovat, to však může přinášet další komplikace).
- *WinRoute* bude pravděpodobně ve většině případů sám sloužit jako DHCP server pro počítače (pracovní stanice) v lokální síti.

Heslo uživatele Admin

Při instalaci je nutné zadat heslo uživatele *Admin* — hlavního správce firewallu. Jméno *Admin* s tímto heslem pak slouží pro přístup:

- Do konzole firewallu (viz kapitola 2.11),
- Ke vzdálené správě firewallu prostřednictvím webového administračního rozhraní (viz kapitola 3),
- Ke vzdálené správě firewallu pomocí aplikace *Kerio Administration Console* (viz kapitola 3).

Zvolené heslo si dobře zapamatujte nebo uložte na bezpečném místě a uchovejte jej v tajnosti!

Nastavení časové zóny, data a času

Pro celou řadu funkcí *WinRoute* (ověřování uživatelů, záznamy, statistiky atd.) je nezbytné správné nastavení data, času a časové zóny na firewallu. Zvolte vaši časovou zónu a v následujícím kroku zkontrolujte, případně upravte nastavení data a času.

Dokončení instalace

Po nastavení všech uvedených parametrů se spustí služba (daemon) *WinRoute Firewall Engine*. Na konzoli firewallu bude po celou dobu jeho běhu zobrazena informace o možnostech vzdálené správy a změny některých základních nastavení — viz kapitola 2.11.

2.8 Upgrade - Software Appliance / VMware Virtual Appliance

Upgrade (aktualizaci) *WinRoute* lze provést dvěma způsoby:

- Spouštěním systému z instalačního CD (resp. připojeného ISO obrazu) nové verze. Instalace probíhá stejným způsobem jako nová instalace, pouze na začátku se instalační program dotáže, zda má být provedena aktualizace (stávající nastavení a data zůstanou zachována) nebo nová instalace (všechny konfigurační soubory, statistiky, záznamy atd. budou vymazány). Podrobnosti viz kapitola 2.7.
- Prostřednictvím kontroly nových verzí v programu *Kerio Administration Console*. Podrobnosti naleznete v kapitole 16.3.

2.9 Komponenty WinRoute

WinRoute sestává z těchto součástí:

WinRoute Firewall Engine
: Vlastní výkonný program, který realizuje všechny služby a funkce. Běží jako služba operačního systému (služba má název *Kerio WinRoute Firewall* a ve výchozím nastavení je spouštěna automaticky pod systémovým účtem).

WinRoute Engine Monitor (pouze Windows)
: 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 2.10.
Poznámka: WinRoute Firewall Engine je zcela nezávislý na aplikaci *WinRoute Engine Monitor*. *Engine* tedy může být spuštěn, i když se na liště právě nezobrazuje ikona.

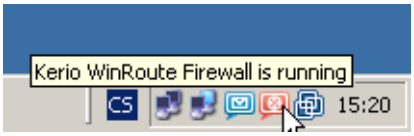
Kerio Administration Console (pouze Windows)
: Univerzální program pro plnou lokální či vzdálenou správu serverových produktů firmy *Kerio Technologies*. Pro připojení k určité aplikaci je potřeba modul obsahující specifické rozhraní pro tuto aplikaci.
Při instalaci *WinRoute* na systém *Windows* je *Kerio Administration Console* nainstalována s příslušným modulem. K dispozici je rovněž samostatný instalační balík *Kerio Administration Console* pro vzdálenou správu *WinRoute* z jiného počítače. Program *Kerio Administration Console* je k dispozici pouze pro systém *Windows*, lze jím však spravovat jak *WinRoute* nainstalovaný na systému *Windows*, tak *Kerio WinRoute Firewall Software Appliance / VMware Virtual Appliance*.
Použití programu *Kerio Administration Console* je podrobně popsáno v samostatném dokumentu *Kerio Administration Console — Nápověda* (http://www.kerio.cz/cz/firewall/manual).

Konzole firewallu (pouze Software Appliance / VMware Virtual Appliance)
: Konzole firewallu je jednoduché rozhraní, které je trvale spuštěné na počítači s *WinRoute*. Umožňuje nastavit základní parametry operačního systému a firewallu, pokud se k němu

nelze vzdáleně přihlásit prostřednictvím rozhraní *Web Administration* ani programu *Kerio Administration Console*.

2.10 WinRoute Engine Monitor (Windows)

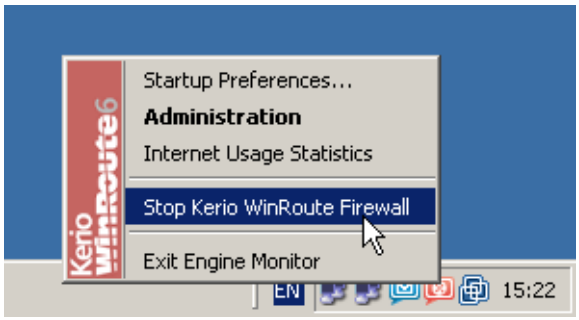
WinRoute Engine Monitor je samostatný program, který slouží k ovládání a sledování stavu *WinRoute Firewall Engine*. Tato komponenta se zobrazuje jako ikona na nástrojové liště.



Obrázek 2.6 Ikona programu WinRoute Engine Monitor v oznamovací oblasti nástrojové lišty

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.

Dvojitým kliknutím levým tlačítkem na tuto ikonu lze spustit program *Kerio Administration Console* (viz dále). Po kliknutí pravým tlačítkem se zobrazí menu s následujícími funkcemi:



Obrázek 2.7 Menu programu WinRoute Engine Monitor

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

Administration
Spuštění programu *Kerio Administration Console* (odpovídá dvojitému kliknutí levým tlačítkem myši na ikonu *WinRoute Engine Monitoru*).

Internet Usage Statistics
Otevření *Statistik využívání Internetu* ve výchozím WWW prohlížeči. Podrobnosti viz kapitola 21.

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

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

Poznámka:

1. 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. *WinRoute Engine Monitor* je k dispozici pouze v anglickém jazyce.

2.11 Konzole firewallu (Software Appliance / VMware Virtual Appliance)

Na konzoli počítače, kde je spuštěn *Kerio WinRoute Firewall Software Appliance / VMware Virtual Appliance*, je po celou dobu jeho běhu zobrazena informace o možnostech vzdálené správy firewallu. Po zadání administrátorského hesla (viz výše) tato konzole umožňuje změnit některá základní nastavení, obnovit výchozí nastavení po instalaci a vypnout nebo restartovat počítač.

Ve výchozím stavu zobrazuje konzole pouze informace o URL, resp. IP adrese, kam se lze připojit ke správě firewallu prostřednictvím webového administračního rozhraní firewallu nebo programu *Kerio Administration Console*. Pro přístup ke konfiguračním volbám je potřeba se nejprve ověřit heslem uživatele *Admin* (hlavního správce firewallu). Při delší době nečinnosti dojde z bezpečnostních důvodů k automatickému odhlášení uživatele a na konzole se opět zobrazí úvodní obrazovka s informacemi o vzdálené správě firewallu.

Konzole firewallu nabízí tyto konfigurační volby:

Konfigurace síťových rozhraní
Tato volba umožňuje zobrazit, případně změnit parametry jednotlivých síťových rozhraní firewallu. Na každém rozhraní lze nastavit automatickou konfiguraci protokolem *DHCP* nebo ručně zadat IP adresu, masku subsítě a výchozí bránu.
Poznámka: Na rozhraních připojených do lokální sítě nesmí být nastavena žádná výchozí brána, jinak nebude možné použít tento firewall jako bránu pro přístup do Internetu.

Nastavení pravidel pro vzdálenou správu
Při změnách komunikačních pravidel firewallu (viz kapitola 7) prostřednictvím webového administračního rozhraní nebo programu *Kerio Administration Console* může dojít k nechtěnému zablokování přístupu ke vzdálené správě.
Pokud jsme si jisti, že síťová rozhraní firewallu jsou nastavena správně, ale přesto se nelze připojit ke vzdálené správě, můžeme volbou *Vzdálená správa* změnit komunikační pravidla firewallu tak, aby neblokovala přístup ke vzdálené správě přes žádné rozhraní.
Po změně komunikačních pravidel bude automaticky restartována služba *Kerio WinRoute Firewall Engine*.

„Odblokování“ vzdálené správy v praxi znamená, že na začátek tabulky komunikačních pravidel bude přidáno pravidlo povolující přístup z libovolného počítače ke službám *KWF Admin* (připojení programem *Kerio Administration Console*), *KWF WebAdmin* (nezabezpečené WWW rozhraní) a *KWF WebAdmin-SSL* (zabezpečené WWW rozhraní).

Vypnutí / restart firewallu

V případě, že potřebujeme firewall vypnout nebo restartovat, tyto volby zajistí bezpečné ukončení služby *Kerio WinRoute Firewall Engine* a vypnutí operačního systému firewallu.

Obnovení továrního nastavení

Tato volba uvede firewall do výchozího stavu jako po spuštění instalace z instalačního CD nebo po prvním spuštění virtuálního zařízení pro *VMware*. Všechny konfigurační soubory a data (záznamy, statistiky atd.) budou vymazány a bude potřeba provést znovu počáteční konfiguraci firewallu, stejně jako při čisté instalaci (viz kapitola 2.7).

Obnovení továrního nastavení může být užitečné v případě, kdy je omylem nebo neodborným zásahem konfigurace firewallu poškozena natolik, že jej již nelze žádnými jinými prostředky znovu zprovoznit.

Kapitola 3

Správa WinRoute

WinRoute nabízí dva nástroje pro konfiguraci:

Rozhraní Web Administration

Rozhraní *Web Administration* umožňuje vzdálenou i lokální správu firewallu prostřednictvím běžného WWW prohlížeče. V současné verzi *WinRoute* umožňuje *Web Administration* konfiguraci nejdůležitějších parametrů *WinRoute*:

- síťových rozhraní,
- komunikačních pravidel,
- pravidel pro filtrování protokolů *HTTP* a *FTP*,
- uživatelských účtů, skupin a domén,
- skupin IP adres, skupin URL, časových intervalů a síťových služeb.

Rozhraní *Web Administration* je dostupné na adrese `https://server:4081/admin` (`server` má význam jména nebo IP adresy firewallu a `4081` je výchozí port jeho WWW rozhraní). Při použití protokolu *HTTPS* je komunikace mezi klientem a *WinRoute Firewall Engine* šifrována, což zabraňuje jejímu odposlechu a zneužití. Nezabezpečenou verzi rozhraní *Web Administration* (protokol *HTTP*) doporučujeme používat pouze pro lokální správu *WinRoute* (tj. správu z počítače, na kterém je nainstalován).

Program Kerio Administration Console

Kerio Administration Console (dále jen „*Administration Console*“) je univerzální aplikace pro správu serverových produktů firmy *Kerio Technologies*. Pro *WinRoute* nabízí všechny konfigurační parametry.

Administration Console umožňuje lokální správu (tj. z téhož počítače, na kterém je *WinRoute* nainstalován) i vzdálenou správu (z libovolného jiného počítače). Komunikace mezi *Administration Console* a *WinRoute Firewall Engine* je šifrována, což zabraňuje jejímu odposlechu a zneužití.

Při instalaci *WinRoute* na systém *Windows* je program *Kerio Administration Console* společně s ním.

K dispozici je rovněž samostatný instalační balík *Kerio Administration Console* pro vzdálenou správu *WinRoute* z jiného počítače. Program *Kerio Administration Console* je k dispozici pouze pro systém *Windows*, lze jím však spravovat jak *WinRoute* nainstalovaný na systému *Windows*, tak *Kerio WinRoute Firewall Software Appliance / VMware Virtual Appliance*.

Použití *Administration Console* je podrobně popsáno v samostatném manuálu *Kerio Administration Console — Nápověda* (tento manuál lze zobrazit volbou *Nápověda* → *Obsah* v hlavním okně *Administration Console* a je rovněž k dispozici v online verzi nebo ke stažení na WWW stránce http://www.kerio.cz/cz/firewall/manual).

Další kapitoly tohoto manuálu popisují jednotlivé sekce programu *Administration Console*, který nabízí všechny dostupné konfigurační možnosti. Koncepce rozhraní *Web Administration* je velmi podobná a jeho jednotlivé části jsou (až na nepatrné odlišnosti) prakticky shodné s příslušnými sekcemi programu *Administration Console*.

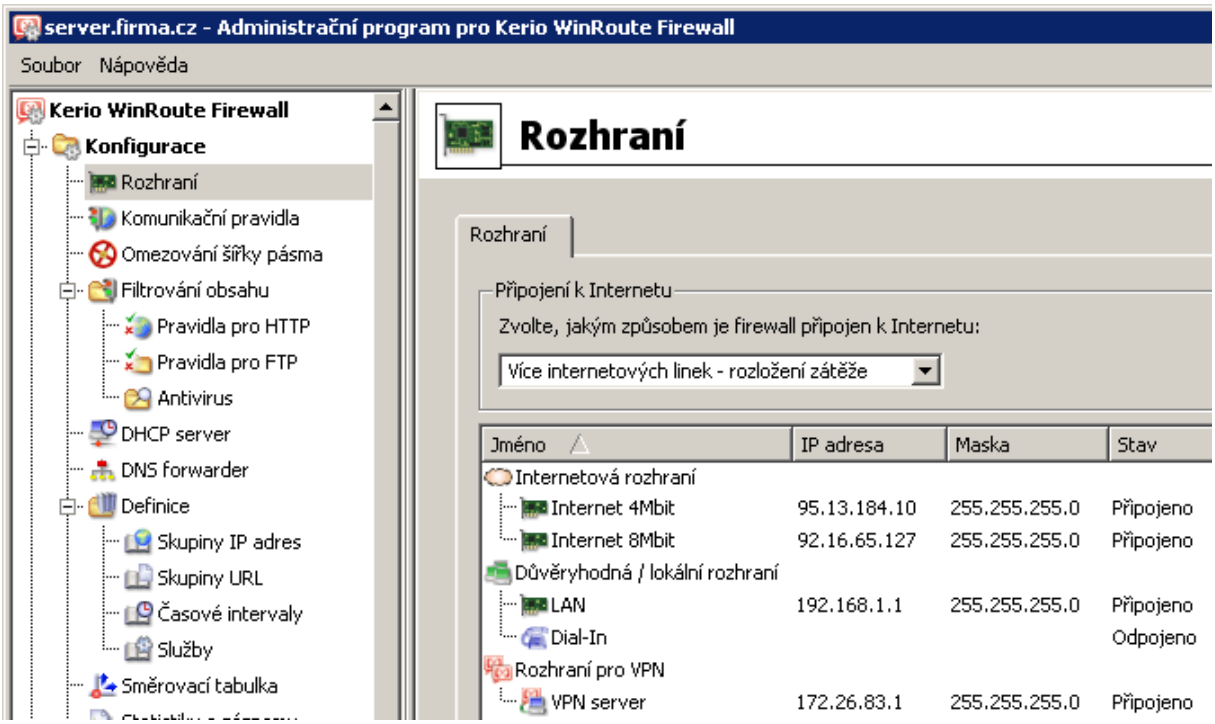
Poznámka:

1. Rozhraní *Web Administration* a program *Administration Console* pro *WinRoute* jsou lokalizovány celkem do 16 jazyků. V rozhraní *Web Administration* lze zvolit jazyk pomocí ikony vlajky v pravém horním rohu okna, případně může být nastaven automaticky podle preferovaného jazyka ve WWW prohlížeči. V programu *Administration Console* lze jazyk zvolit v přihlašovacím okně v nabídce *Nástroje*.

2. Při prvním přihlášení do programu *Administration Console* po instalaci *WinRoute* se nejprve automaticky spustí průvodce vytvořením komunikačních pravidel, který slouží k počáteční konfiguraci *WinRoute*. Podrobný popis tohoto průvodce naleznete v kapitole 7.1.

3.1 Administration Console - hlavní okno

Po úspěšném přihlášení programem *Administration Console* k *WinRoute Firewall Engine* se zobrazí okno modulu pro správu *WinRoute* (dále jen „administrační okno“). Toto okno je rozděleno na dvě části:



Obrázek 3.1 Hlavní okno Administration Console pro WinRoute

- Levý sloupec obsahuje seznam sekcí administračního okna v podobě stromu. Pro větší přehlednost lze jednotlivé části stromu skrývat a rozbalovat. *Administration Console* si při svém ukončení zapamatuje aktuální nastavení stromu a při dalším přihlášení jej zobrazí ve stejné podobě.
- Pravá část okna zobrazuje obsah sekce zvolené v levém sloupci (případně seznam sekcí ve zvolené skupině).

Hlavní menu administračního okna

Hlavní menu obsahuje tyto funkce:

Nabídka Soubor

- *Obnovit připojení* — připojení k *WinRoute Firewall Engine* po výpadku spojení (např. z důvodu restartu *Engine* či síťové chyby).
- *Nové připojení* — otevření (resp. přepnutí do) hlavního okna *Administration Console*. V tomto okně se pak můžeme pomocí záložky nebo přihlašovacího dialogu připojit k požadovanému serveru.
  Tuto funkci lze využít, pokud chceme spravovat více serverových aplikací současně (např. *WinRoute* na více serverech). Podrobnosti viz manuál *Administration Console — Nápověda*.
  Poznámka: Volba *Připojit k novému serveru* má zcela identický efekt jako spuštění *Administration Console* z nabídky *Start*.
- *Konec* — ukončení správy (odhlášení od serveru a uzavření administračního okna). Stejného efektu dosáhneme uzavřením okna kliknutím na závěr (křížek) v pravém horním rohu nebo kombinací kláves *Alt+F4* či *Ctrl+Q*.

Nabídka Změnit (pouze na úvodní obrazovce)

Volby v nabídce *Změnit* souvisejí s licencí a registrací produktu. Dostupné volby se mění v závislosti na stavu registrace (např. pokud je produkt již zaregistrován jako zkušební verze, pak lze provést pouze registraci zakoupené verze nebo změnu registračních údajů).

- *Zkopírovat licenční číslo do schránky* — zkopírování čísla aktuální licence (položka *ID licence*) do schránky. Toto může být užitečné např. při objednávce upgrade nebo předplatného, kdy je třeba zadat číslo základní licence, nebo při zadávání požadavku na technickou podporu *Kerio Technologies*.
- *Zaregistrovat zkušební verzi* — registrace zkušební verze produktu.
- *Zaregistrovat produkt* — registrace produktu se zakoupeným licenčním číslem.
- *Instalovat licenci* — import souboru s licenčním klíčem (podrobnosti viz kapitola 4.4).

Nabídka Nápověda

- *Zobrazit identitu serveru* — informace o firewallu, ke kterému je *Administration Console* aktuálně připojena (jméno nebo IP adresa serveru, port a otisk SSL certifi-

kátu). Tyto informace lze využít pro ověření identity firewallu při přihlašování ke správě z jiného počítače (viz manuál *Kerio Administration Console — Nápověda*).
- *Příručka administrátora* — otevření příručky administrátora (tohoto manuálu) ve formátu *HTML Help*. Podrobnosti o nápovědách naleznete v manuálu *Kerio Administration Console — Nápověda*.
- *O aplikaci* — informace o verzi aplikace (v tomto případě administračního modulu pro *WinRoute*), odkaz na WWW stránku výrobce a další informace.

Stavový řádek

Na dolním okraji administračního okna je umístěn stavový řádek, který zobrazuje tyto informace (v pořadí zleva doprava):

Obrázek 3.2 Stavový řádek okna Administration Console

- Aktuální sekce administračního okna (vybraná v levém sloupci). Tato informace usnadňuje orientaci v administračním okně zejména v případech, kdy není vidět celý strom sekcí (např. při nižším rozlišení obrazovky).
- Jméno nebo IP adresa serveru a port serverové aplikace (*WinRoute* používá port 44333).
- Jméno uživatele přihlášeného ke správě.
- Aktuální stav *Administration Console*: *Připraven* (čekání na akci uživatele), *Načítání* (přenos dat ze serveru) nebo *Ukládání* (zápis provedených změn na server).

Detekce výpadku připojení k WinRoute Firewall Engine

Administration Console dokáže automaticky detekovat, že došlo k výpadku připojení. Výpadek je zpravidla detekován při pokusu o čtení nebo uložení dat z/na server (tj. při stisknutí tlačítka *Použít* nebo přepnutí do jiné sekce *Administration Console*). V takovém případě se automaticky zobrazí dialog pro obnovení připojení s příslušným chybovým hlášením.

Po odstranění příčiny výpadku můžeme zkusit připojení obnovit. *Administration Console* nabízí dvě možnosti:

- *Použít & Obnovit připojení* — spojení se serverem bude obnoveno a poté budou uloženy všechny změny provedené v aktuální sekci *Administration Console* před výpadkem připojení,
- *Obnovit připojení* — spojení se serverem bude obnoveno, ale provedené změny budou stornovány.

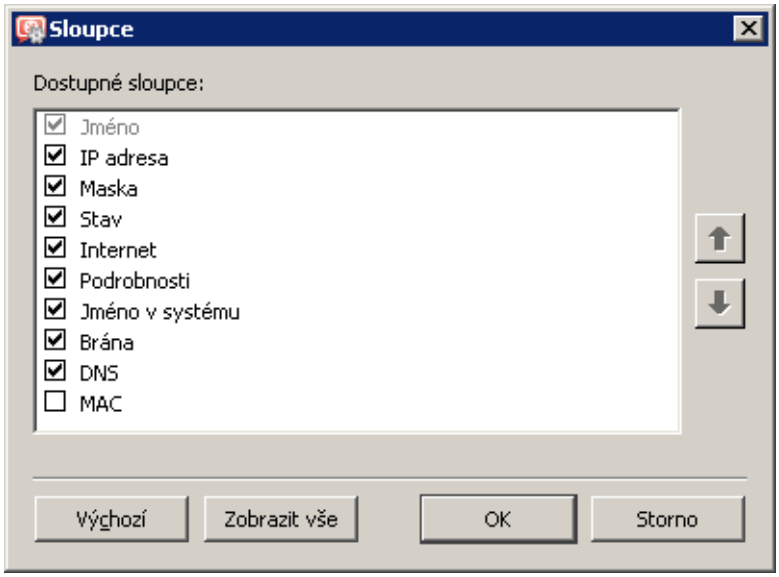
Pokud se připojení nepodaří obnovit, zobrazí se již pouze chybové hlášení. Pak můžeme zkusit připojení obnovit volbou *Soubor* → *Obnovit připojení* z hlavního menu, případně okno uzavřít a připojit se znovu standardním způsobem.

Poznámka: Rozhraní *Web Administration* po výpadku a obnovení připojení automaticky přejde na přihlašovací stránku. Případné neuložené změny budou ztraceny.

3.2 Administration Console - nastavení pohledů

V mnoha sekcích *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 výše popsaných 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.



Obrázek 3.3 Výběr zobrazovaných sloupců v sekci Rozhraní

Dialog obsahuje seznam všech sloupců dostupných v příslušném pohledu. Zaškrtávací pole (vlevo od názvu sloupce) zapíná/vypíná zobrazování tohoto sloupce. Tlačítko *Zobrazit vše* nastavuje zobrazování všech dostupných sloupců. Tlačítko *Výchozí* uvede nastavení sloupců do výchozího stavu (ve výchozím nastavení jsou zpravidla z důvodu přehlednosti zobrazeny pouze sloupce s nejdůležitějšími informacemi, zatímco sloupce s doplňujícími informacemi jsou skryty).

Tlačítka se šipkami slouží k posunu vybraného sloupce v seznamu nahoru nebo dolů. Tím lze určit pořadí, v jakém mají být sloupce zobrazeny.

Pořadí sloupců lze také upravit v pohledu samotném: klikneme levým tlačítkem myši na název sloupce, podržíme jej a přesuneme na požadované místo.

Poznámka: Šířku jednotlivých sloupců lze upravit posunutím dělicích čar mezi záhlavími sloupců.

Kapitola 4

Registrace produktu a licence

Zakoupený produkt *Kerio WinRoute Firewall* je třeba zaregistrovat, čímž dojde k vytvoření tzv. licenčního klíče(soubor `license.key` — viz kapitola 25.1). 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 je zaregistrována či nikoliv. Každý zákazník má tak možnost si produkt ve třicetidenní lhůtě vyzkoušet v konkrétních podmínkách. Pokud si jej zakoupí, stačí pouze zaregistrovat nainstalovanou verzi se zakoupeným licenčním číslem (viz kapitola 4.3). Není tedy třeba *WinRoute* znovu instalovat a nastavovat.

V případě, že třicetidenní zkušební lhůta již vypršela, *WinRoute* omezí rychlost veškeré síťové komunikace počítače, na kterém je nainstalován, na 4 KB/s. Rovněž zablokuje směrování (tzn. počítač s *WinRoute* pak nemůže sloužit jako brána do Internetu). Po registraci s platným licenčním číslem (získaným při zakoupení produktu) je *WinRoute* opět funkční v plném rozsahu.

Poznámka: Dojde-li ke ztrátě licenčního klíče (např. z důvodu havárie disku, nechtěným smazáním apod.), stačí produkt jednoduše znovu zaregistrovat s prodejním číslem základního produktu. Stejným způsobem lze postupovat při změně platformy firewallu (*Windows / Software Appliance / VMware Virtual Appliance*) — licenční klíč je nepřenositelný mezi platformami. Při ztrátě licenčního čísla je nutné kontaktovat obchodní oddělení společnosti *Kerio Technologies*.

4.1 Typy licencí a počet uživatelů

Typy licencí (volitelné komponenty)

WinRoute může obsahovat volitelné komponenty: antivirový program *McAfee* (viz kapitola 13) a modul pro hodnocení obsahu WWW stránek *Kerio Web Filter* (viz kapitola 12.3). Tyto komponenty jsou licencovány odděleně.

Licenční klíč 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.
- skončení funkčnosti antivirového modulu — po tomto datu se antivirový modul *McAfee* zablokuje a nelze jej nadále používat.

Upozornění

Vzhledem ke stálému výskytu nových virů doporučujeme používat vždy nejnovější verzi virové databáze.

Předplatné modulu Kerio Web Filter

Modul *Kerio Web Filter* je dodáván jako služba. Licence je určena pouze datem skončení platnosti, po kterém přestane tento modul fungovat.

Poznámka: Aktuální informace o jednotlivých licencích, možnostech prodloužení jejich platnosti atd. naleznete na WWW stránkách firmy *Kerio Technologies* (http://www.kerio.cz/).

Stanovení potřebného počtu uživatelů

Součástí licenčního klíče pro *WinRoute* je informace o maximálním povoleném počtu uživatelů. Dle licenčních podmínek počet uživatelů znamená počet počítačů, které *WinRoute* chrání, tj. součet:

- všech počítačů v lokální síti (pracovních stanic i serverů),
- všech (potenciálních) VPN klientů připojujících se z Internetu do lokální sítě.

Do celkového počtu uživatelů se nezahrnuje počítač, na kterém je *WinRoute* nainstalován.

Upozornění

Při překročení maximálního povoleného počtu uživatelů bude *WinRoute* blokovat komunikaci některých počítačů!

4.2 Informace o licenci

Informace o licenci lze zobrazit volbou *Kerio WinRoute Firewall* (první položka ve stromu v levé části okna *Administration Console* — tato sekce se zobrazuje bezprostředně po přihlášení ke správě *WinRoute*).

Obrázek 4.1 Úvodní stránka Administration Console s informacemi o licenci

Produkt
Název produktu (*Kerio WinRoute Firewall*).

Copyright
Informace o držiteli autorských práv.

Domovská stránka
Odkaz na domovskou stránku produktu *Kerio WinRoute Firewall* (informace o cenách, nových verzích atd.). Kliknutím na odkaz se domovská stránka otevře ve WWW prohlížeči, který je v operačním systému nastaven jako výchozí.

Operační systém
Název operačního systému, na kterém běží služba *WinRoute Firewall Engine*. Tento údaj je pouze informativní — zakoupená licence je platná pro libovolný podporovaný operační systém.

ID licence
Licenční číslo nebo označení speciální licence.

Právo na aktualizaci končí
Datum skončení nároku na bezplatný upgrade produktu.

Funkčnost produktu končí
Datum skončení funkčnosti produktu (pouze u zkušební verze nebo speciálních licencí).

Počet uživatelů
Maximální počet počítačů (unikátních IP adres), které může *WinRoute* chránit (podrobnosti viz kapitola 4.6).

Společnost
Název společnosti (příp. osoby), na niž je produkt registrován.

V závislosti na aktuální licenci se v dolní části obrázku zobrazují odkazy:

1. V případě neregistrované verze:
   - *Zaregistrovat se jako uživatel zkušební verze* — registrace zkušební verze produktu. Tato registrace je nepovinná a nezávazná. Registrací získá uživatel nárok na bezplatnou technickou podporu po dobu zkušebního období.
   - *Zaregistrovat produkt se zakoupeným licenčním číslem* — registrace zakoupeného produktu.
     Zakoupený produkt je nutno zaregistrovat, jinak se bude stále chovat jako zkušební verze!

2. V případě registrované verze:
   - *Aktualizovat registrační informace* — možnost úpravy údajů o firmě/osobě, na kterou je produkt registrován, nebo přidání licenčních čísel předplatného či add-on licencí (zvýšení počtu uživatelů).

Ve všech případech bude spuštěn průvodce registrací, který uživatele vyzve k zadání potřebných a doplňujících údajů. Podrobnosti o tomto průvodci naleznete v kapitole 4.3.

Je-li aktivní automatická kontrola nových verzí (viz kapitola 16.3), pak se v případě zveřejnění nové verze zobrazí odkaz *K dispozici je nová verze programu. Klikněte zde pro podrobnosti...*. Po kliknutí na tento odkaz se otevře dialog umožňující stažení nové verze a následné spuštění instalace (podrobnosti viz kapitola 16.3).

Poznámka: Po kliknutí pravým tlačítkem myši na úvodní stránce *Administration Console* se zobrazí kontextové menu s volbami odpovídající nabídce *Změnit* v hlavním menu administračního okna (viz kapitola 3.1).

4.3 Registrace produktu z Administration Console

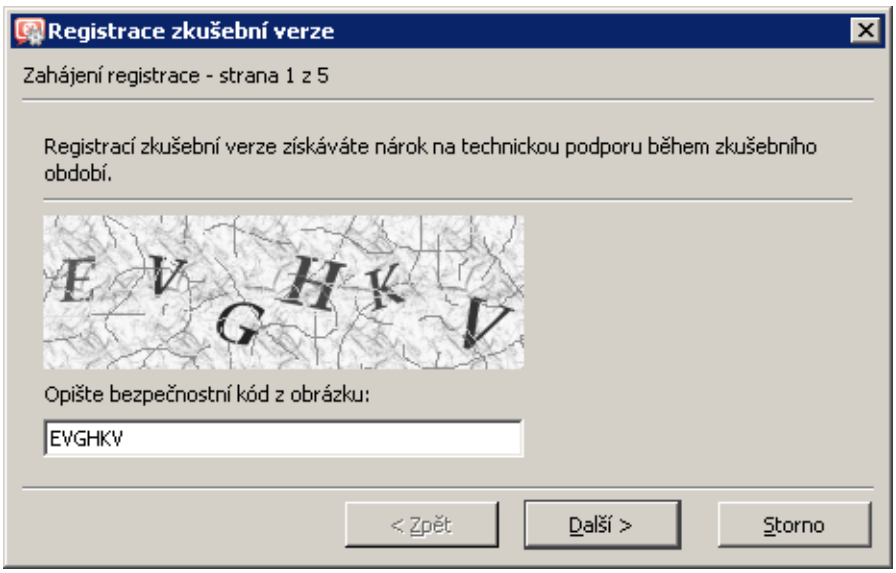
Registraci *WinRoute*, změnu registračních údajů, přidání add-on licencí nebo prodloužení předplatného lze provést přímo z *Administration Console* kliknutím na příslušný odkaz v úvodní obrazovce (viz kapitola 4.2), případně odpovídající volbou z nabídky *Změnit* v hlavním menu administračního okna (viz kapitola 3.1).

Registrace zkušební verze

Registrací zkušební verze získá uživatel e-mailovou a telefonickou technickou podporu zdarma po dobu zkušební periody. Zároveň společnost *Kerio Technologies* získává zpětnou vazbu od těchto uživatelů. Registrace zkušební verze je nepovinná, ale doporučená (přináší pouze výhody). Registrace *nezavazuje* uživatele ke koupi produktu.

Kliknutím na odkaz *Zaregistrovat se jako uživatel zkušební verze* se spustí průvodce registrací.

1. V prvním kroku průvodce je třeba opsat bezpečnostní kód z obrázku do textového pole (ochrana proti zneužití registračního serveru). V bezpečnostním kódu se nerozlišují malá a velká písmena.

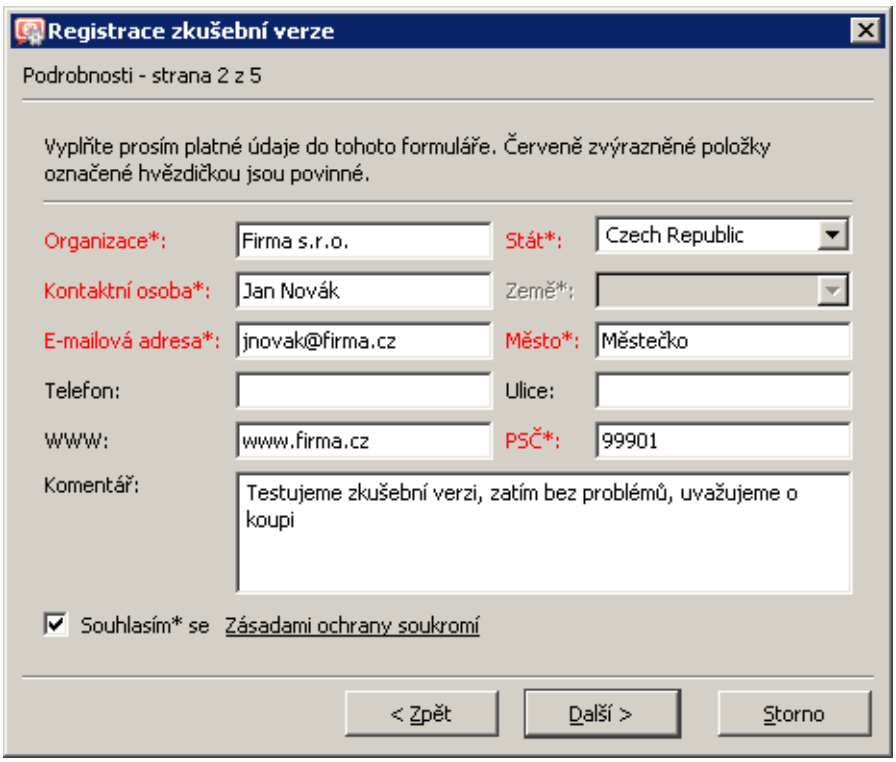


Obrázek 4.2 Registrace zkušební verze — bezpečnostní kód

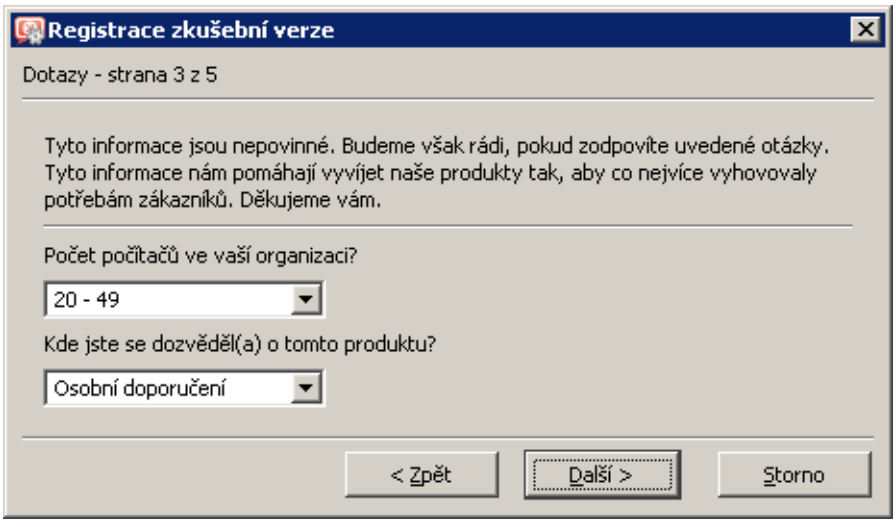
2. Ve druhém kroku je třeba vyplnit údaje o uživateli zkušební verze (osobě, firmě). Důležitý je také souhlas uživatele se *Zásadami ochrany soukromí* — bez tohoto souhlasu nemohou být zadané údaje uloženy do databáze společnosti *Kerio Technologies*.

   Do položky *E-mailová adresa* je nutno uvést platnou e-mailovou adresu, nejlépe přímo adresu osoby, která registraci provádí. Na tuto adresu bude po dokončení průvodce zaslána žádost o potvrzení registrace.

3. Třetí krok průvodce obsahuje nepovinné doplňující otázky. Odpovědi na tyto otázky pomáhají společnosti *Kerio Technologies* v zacílení produktu na správnou skupinu zákazníků.



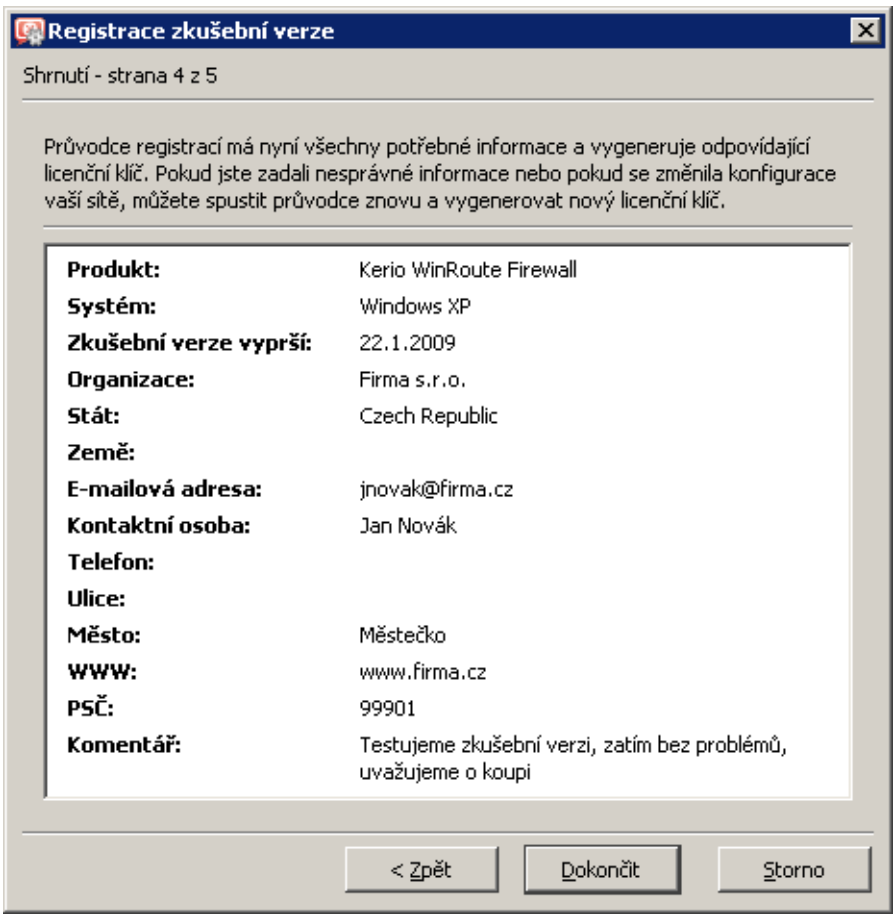
Obrázek 4.3 Registrace zkušební verze — údaje o uživateli



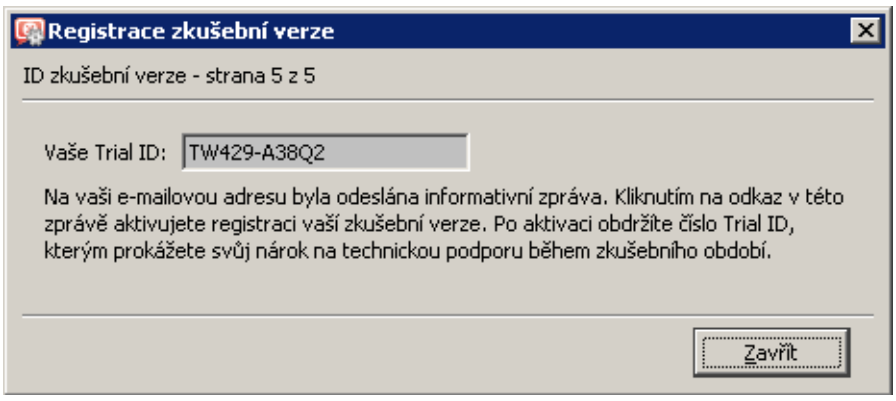
Obrázek 4.4 Registrace zkušební verze — doplňující otázky

4. Ve čtvrtém kroku se zobrazí shrnutí zadaných údajů. Je-li některý údaj nesprávný, lze se tlačítkem *Zpět* vrátit do příslušného kroku průvodce a opravit jej.

5. V posledním kroku průvodce se zobrazí příslušné *Trial ID*. Toto je jedinečný identifikátor registrované zkušební verze, kterým se registrovaný uživatel prokazuje v případě požadavku na technickou podporu.



Obrázek 4.5 Registrace zkušební verze — shrnutí



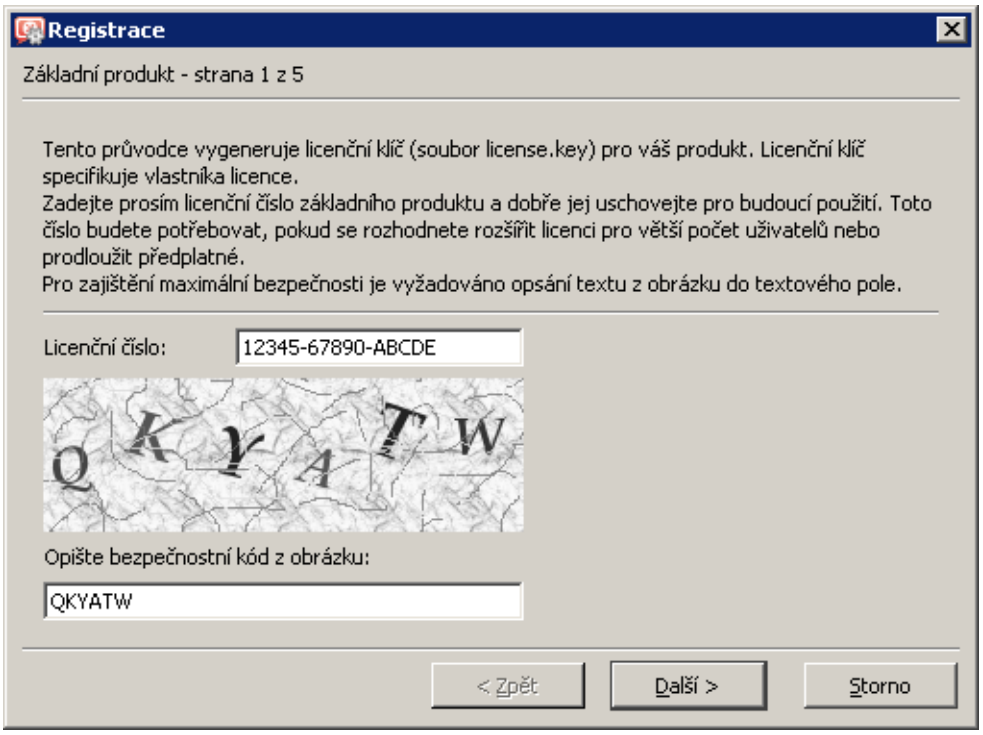
Obrázek 4.6 Registrace zkušební verze — Trial ID

Na e-mailovou adresu uvedenou ve druhém kroku průvodce se v tomto okamžiku odešle žádost o potvrzení registrace (v jazyce odpovídajícím jazyku *Administration Console*). Teprve po kliknutí na odkaz v této zprávě je registrace dokončena a příslušné *Trial ID* platné. Hlavním účelem tohoto potvrzení je ověření platnosti e-mailové adresy uvedené při registraci.

Registrace zakoupeného produktu

Kliknutím na odkaz *Zaregistrovat produkt se zakoupeným licenčním číslem* se spustí průvodce registrací.

1. V prvním kroku průvodce je třeba zadat patnáctimístné licenční číslo základního produktu (získané při jeho zakoupení) a opsat bezpečnostní kód z obrázku do textového pole (ochrana proti zneužití registračního serveru). V licenčním čísle ani v bezpečnostním kódu se nerozlišují malá a velká písmena.



Obrázek 4.7 Registrace zakoupeného produktu — číslo základního produktu a bezpečnostní kód

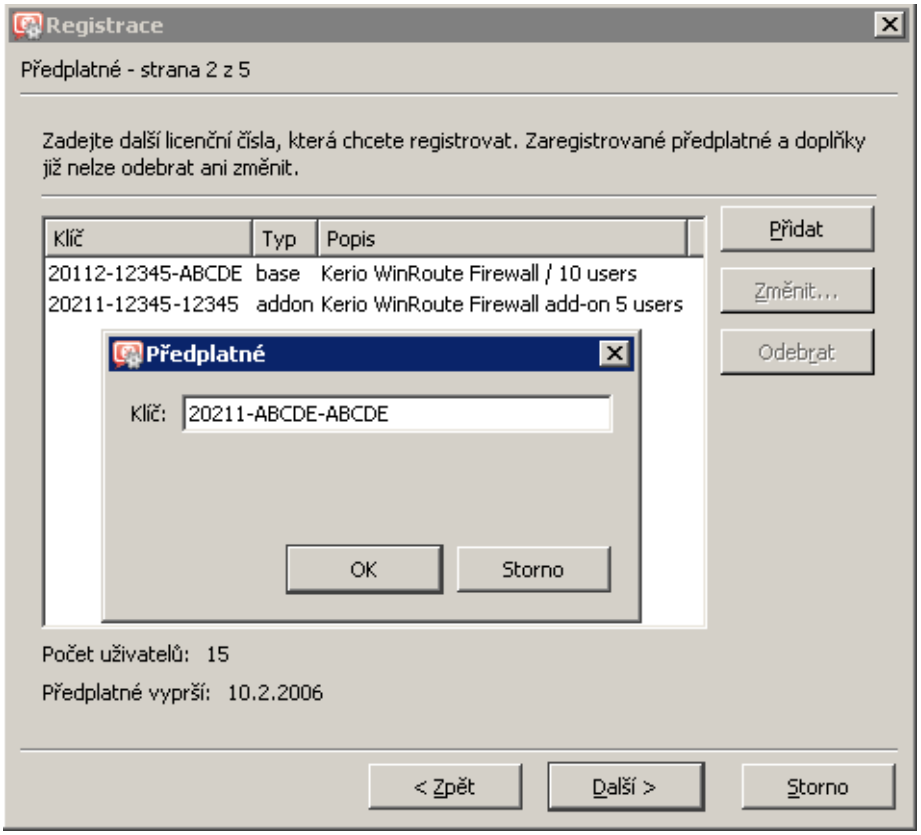
2. Ve druhém kroku lze zadat případná licenční čísla add-on licencí (zvýšení počtu uživatelů), volitelných doplňků nebo předplatného. Zároveň zde budou zobrazena všechna taková licenční čísla, která byla k příslušnému základnímu produktu již dříve zaregistrována.

   Tlačítkem *Přidat* lze přidávat další zakoupená licenční čísla. Každé zadané číslo je ihned zkontrolováno — přidat lze pouze platné licenční číslo.

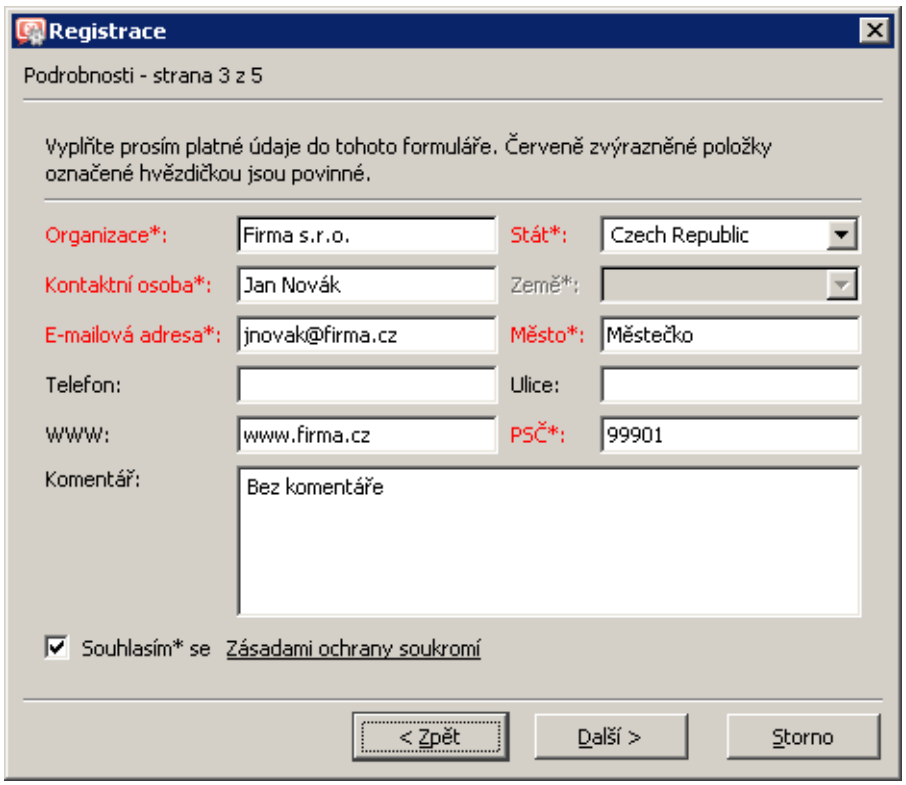
   Nově zadaná licenční čísla lze v případě potřeby změnit nebo odebrat. Zaregistrovaná licenční čísla (z předchozích registrací) již odebrat nelze.

3. Ve třetím kroku je třeba vyplnit údaje o uživateli (osobě, firmě). Důležitý je také souhlas uživatele se *Zásadami ochrany soukromí* — bez tohoto souhlasu nemohou být zadané údaje uloženy do databáze společnosti *Kerio Technologies*.

   Do položky *E-mailová adresa* je nutno uvést platnou e-mailovou adresu, nejlépe přímo adresu osoby, která registraci provádí. Na tuto adresu bude po dokončení průvodce zaslána žádost o potvrzení registrace.



Obrázek 4.8 Registrace zakoupeného produktu — licenční čísla doplňků, add-on licencí a předplatného



Obrázek 4.9 Registrace zakoupeného produktu — údaje o uživateli

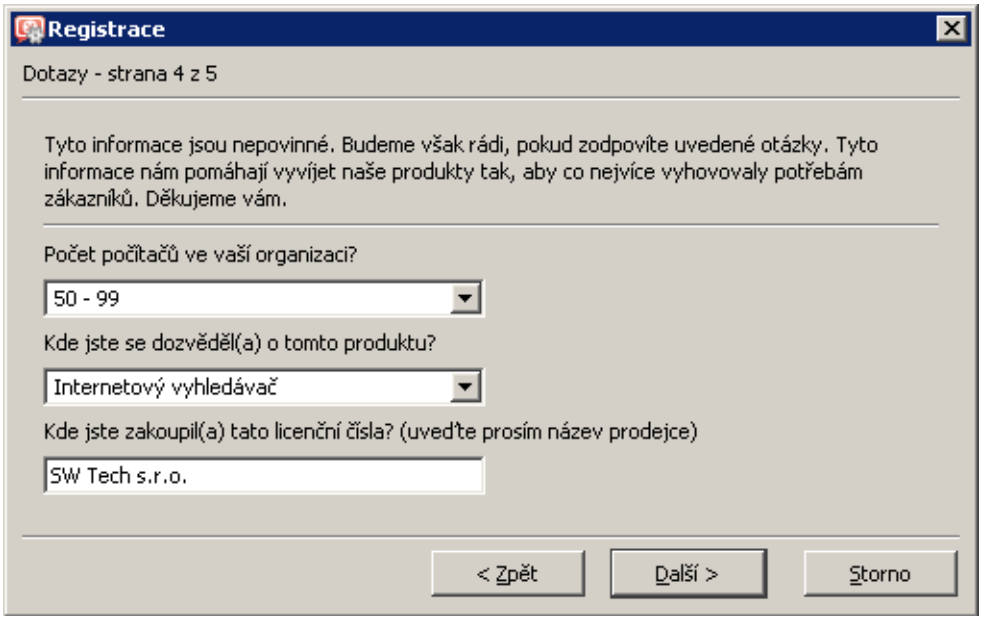
4. Čtvrtý krok průvodce obsahuje nepovinné doplňující otázky. Odpovědi na tyto otázky pomáhají společnosti *Kerio Technologies* v zacílení produktu na správnou skupinu zákazníků.

   Tyto otázky se zobrazují pouze při prvotní registraci. Pokud byly již zodpovězeny, pak se tento krok průvodce nezobrazí (průvodce pak má pouze čtyři kroky).

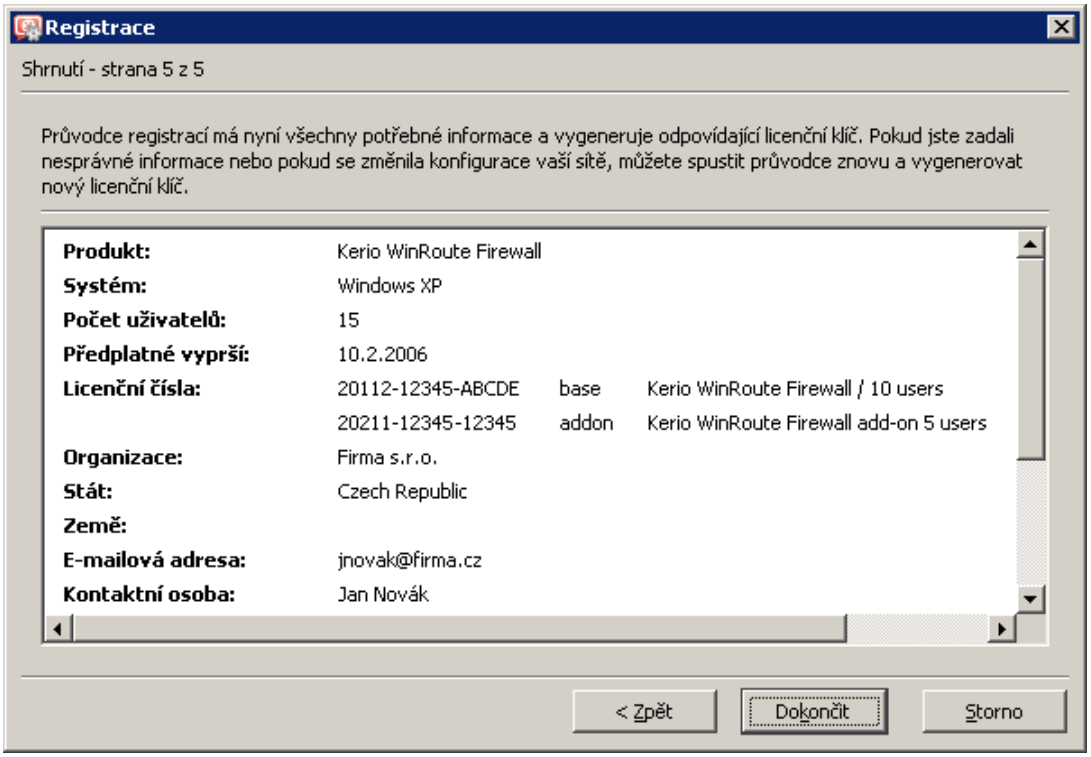
5. V posledním kroku se zobrazí shrnutí zadaných údajů. Je-li některý údaj nesprávný, lze se tlačítkem *Zpět* vrátit do příslušného kroku průvodce a opravit jej.

   Po stisknutí tlačítka *Dokončit* se na základě zadaných údajů automaticky vygeneruje příslušný licenční klíč. Nová licence je ihned aktivní (není vyžadován žádný restart).

   Poznámky:



Obrázek 4.10 Registrace zakoupeného produktu — doplňující otázky



Obrázek 4.11 Registrace zakoupeného produktu — shrnutí

1. Vytvořený licenční klíč je určen pouze pro operační systém, na kterém byl *WinRoute* nainstalován v době registrace (*Windows / Linux*). Licence sama o sobě je přenositelná, ale licenční klíč je vygenerován vždy pro konkrétní platformu.

2. Pokud je po dokončení průvodce hlášena chyba (např. z důvodu výpadku sítě apod.),

stačí spustit průvodce znovu a zopakovat registrační proces.

4.4 Registrace produktu na WWW stránkách

Pokud z nějakého důvodu nelze provést registraci *WinRoute* z *Administration Console*, pak je možné produkt zaregistrovat na WWW stránkách *Kerio Technologies*. Registrační formulář otevřete volbou *Podpora* → *Zaregistrovat licenci* z hlavní nabídky.

Formulář je velmi podobný průvodci registrací popsanému v kapitole 4.3. Po vyplnění registračního formuláře bude automaticky vygenerován soubor s příslušným licenčním klíčem.

Při vyplňování registračních údajů zvolte správně operační systém, na kterém chcete vaši licenci používat (*Windows* nebo *Linux*). Licence sama o sobě je přenositelná, ale licenční klíč je již určen pouze pro konkrétní platformu.

Instalace licenčního klíče

Licenční klíč lze nainstalovat dvěma způsoby:

- Volbou *Instalovat licenci* z nabídky *Změnit* v hlavním menu administračního okna (viz kapitola 3.1). Tento odkaz zobrazí standardní systémový dialog pro otevření souboru. Je-li instalace licenčního klíče úspěšná, licence je ihned aktivní. Na úvodní stránce *Administration Console* se zobrazí se informace o nové licenci.
  Tímto způsobem lze instalovat licenční klíč i vzdáleně (soubor s licenčním klíčem musí být uložen na disku počítače, ze kterého je vzdálená správa prováděna).
- Zkopírováním souboru s licenčním klíčem do příslušného adresáře.
  Licenční klíč je třeba uložit do podadresáře `license` instalačního adresáře *WinRoute* (typicky `C:\Program Files\Kerio\WinRoute Firewall\license`).
  Název souboru (`license.key`) musí zůstat zachován!
  Pro aktivaci licence je nutné restartovat (zastavit a znovu spustit) *WinRoute Firewall Engine*.

Poznámka: Je-li to možné, doporučujeme registrovat *WinRoute* prostřednictvím *Administration Console* (není nutný restart *WinRoute Firewall Engine*).

4.5 Vypršení licence nebo práva na aktualizaci

WinRoute automaticky upozorňuje správce na blížící se datum skončení platnosti licence *WinRoute*, antiviru *McAfee* nebo modulu *Kerio Web Filter* a/nebo skončení práva na aktualizaci (tzv. předplatného)*WinRoute* nebo antiviru *McAfee*. Hlavním účelem těchto upozornění je včas informovat správce tom, že je třeba prodloužit předplatné *WinRoute* nebo obnovit příslušnou licenci.

Tato upozornění mají dvě podoby:

- Upozornění bublinovou zprávou (tyto zprávy zobrazuje komponenta *WinRoute Engine Monitor*),
- Upozornění informačním oknem po přihlášení do *Administration Console* (pouze na vypršení předplatného).

Poznámka: Správce *WinRoute* může rovněž nastavit zasílání výstrahy o vypršení licence nebo předplatného formou e-mailu nebo krátké textové zprávy na mobilní telefon (viz kapitola 19.4).

Upozornění bublinovými zprávami (Windows)

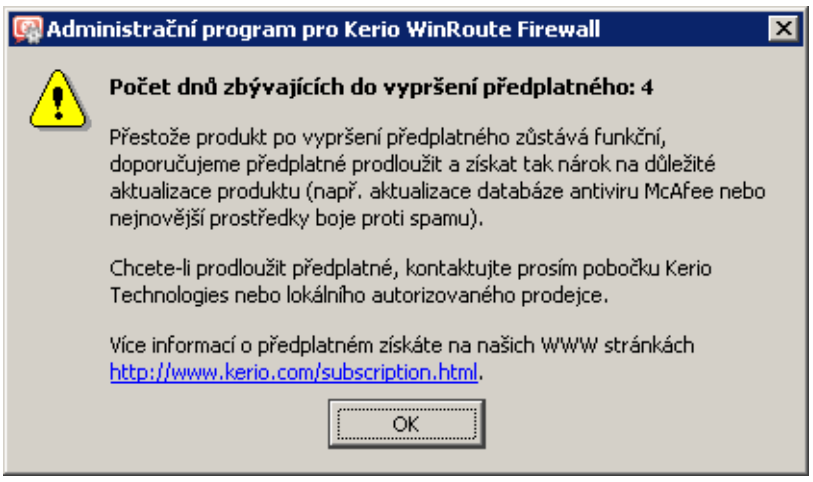
Sedm dní před inkriminovaným datem začne *WinRoute Engine Monitor* periodicky (několikrát denně) zobrazovat informaci o tom, kolik dní zbývá do vypršení licence nebo předplatného.

Tato informace se zobrazuje až do chvíle, kdy přestane být *WinRoute* nebo některá z jeho komponent funkční, případně kdy vyprší předplatné *WinRoute* nebo antiviru *McAfee*. Informace se rovněž přestane zobrazovat bezprostředně po registraci předplatného nebo licence příslušné komponenty (podrobnosti viz kapitola 4.3).

Upozornění v Administration Console

Počínaje 30. dnem před vypršením předplatného se po každém přihlášení zobrazí varování o zbývajícím počtu dnů do vypršení, případně že předplatné již vypršelo. Součástí tohoto upozornění je odkaz na WWW stránky společnosti *Kerio Technologies*, kde lze získat bližší informace o předplatném a objednat předplatné na další období.

Upozornění se přestane zobrazovat po registraci licenčního čísla nového předplatného (viz kapitola 4.3).



Obrázek 4.12 Upozornění na blížící se vypršení předplatného

4.6 Kontrola počtu uživatelů

Tato kapitola podrobně popisuje způsob, jakým *WinRoute* kontroluje, zda nedošlo k překročení počtu uživatelů povoleného licencí.

Licence *WinRoute* neomezuje počet uživatelských účtů. Skutečný počet vytvořených účtů neovlivňuje počet využitých licencí.

Upozornění

Následující popis slouží pouze jako technická informace, kterou lze použít např. při řešení problémů. Při určování potřebného počtu uživatelů (pro nákup licence) je nutné respektovat licenční podmínky — viz kapitola 4.1!

Kontrola využití licence probíhá takto:

Start WinRoute

Při startu *WinRoute* obsahuje tabulka klientů pouze firewall. Počet využitých licencí je roven nule.

Poznámka: Tabulka klientů se zobrazuje v *Administration Console* v sekci *Aktivní počítače* — viz kapitola 19.1.

Čerpání licencí

Při zachycení komunikace jakéhokoliv klienta *WinRoute* zkontroluje, zda pro jeho IP adresu již existuje záznam v tabulce klientů. Pokud ne, přidá do tabulky nový záznam a zvýší počet využitých licencí o 1.

Za klienty jsou považovány:

1. Všechny počítače, ze kterých jsou uživatelé přihlášeni k firewallu
2. Všichni klienti proxy serveru ve *WinRoute* (viz kapitola 8.4)
3. Všechny počítače v lokální síti, jejichž komunikace je směrována mezi internetovými a lokálními rozhraními *WinRoute*. Do této skupiny patří:
    - Každý počítač, který přistupuje do Internetu, ale není z něj přihlášen žádný uživatel,
    - Všechny lokální servery zpřístupněné (mapované) z Internetu,
    - Všichni VPN klienti připojení z Internetu do lokální sítě.

Čerpání licencí neovlivňují:

- DNS dotazy obsluhované modulem *DNS* (pozor: používají-li klienti DNS server umístěný mimo lokální síť, pak se jedná o komunikaci do Internetu),
- DHCP komunikace (může být použit modul *DHCP server* ve *WinRoute* nebo jiný DHCP server na počítači s *WinRoute*),
- Lokální komunikace s firewallem (např. přístup ke sdíleným diskům) počítačů, ze kterých není k firewallu přihlášen žádný uživatel.

Uvolňování licencí

Pro každý záznam v tabulce klientů je sledována doba nečinnosti (tj. doba, po kterou není zachycen žádný paket s odpovídající IP adresou vyhovující výše uvedeným podmínkám). Dosáhne-li doba nečinnosti některého klienta 15 minut, příslušný záznam je z tabulky odstraněn a počet využitých licencí snížen o 1. Uvolněnou licenci může případně využít jiný počítač.

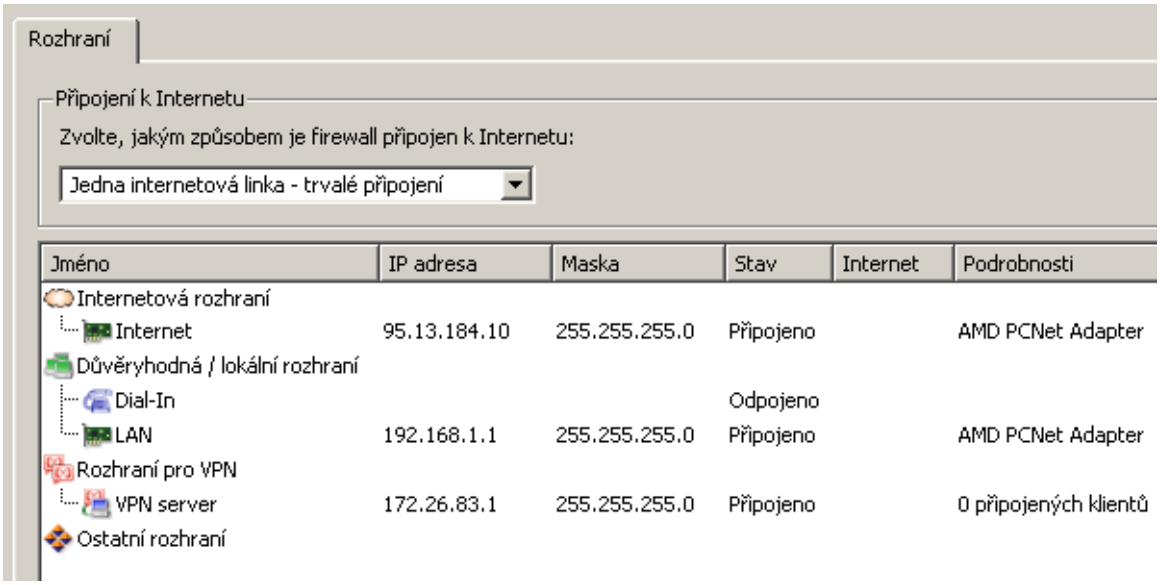
Kapitola 5

Síťová rozhraní

WinRoute je síťový firewall. To znamená, že tvoří bránu mezi dvěma nebo více sítěmi (typicky mezi lokální sítí a Internetem) a obsluhuje komunikaci procházející přes síťová rozhraní (*Ethernet*, *WiFi*, vytáčené linky atd.), která jsou do těchto sítí připojena.

WinRoute v principu pracuje jako IP směrovač nad všemi síťovými rozhraními, která jsou v systému instalována.[3] Základem konfigurace firewallu je proto správné nastavení síťových rozhraní.

Síťová rozhraní firewallu lze rozhraní zobrazit a konfigurovat v programu *Administration Console* nebo v rozhraní *Web Administration* v sekci *Konfigurace* → *Rozhraní*.



Obrázek 5.1 Síťová rozhraní

Skupiny rozhraní

Pro snazší konfiguraci firewallu a lepší přehlednost se síťová rozhraní ve *WinRoute* řadí do skupin. V komunikačních pravidlech firewallu lze skupiny rozhraní použít v položkách *Zdroj* a *Cíl*, stejně jako jednotlivá rozhraní (podrobnosti viz kapitola 7.3). Hlavní výhodou skupin rozhraní je fakt, že při změně internetového připojení, přidání nové linky, výměně síťového

[3] Chceme-li docílit toho, aby *WinRoute* nepracoval s některým rozhraním, je možné ve vlastnostech tohoto rozhraní vypnout komponentu *Kerio WinRoute Firewall* (nízkoúrovňový ovladač *WinRoute*). Z důvodu zajištění bezpečnosti a plné kontroly nad síťovou komunikací procházející přes firewall však doporučujeme nevypínat nízkoúrovňový ovladač *WinRoute* na žádném síťovém rozhraní!

adaptéru atd. není vůbec nutné zasahovat do komunikačních pravidel — stačí pouze zařadit nové rozhraní do správné skupiny.

Ve *WinRoute* jsou definovány tyto skupiny rozhraní:

- *Internetová rozhraní* — rozhraní, která jsou nebo mohou být použita pro připojení k Internetu (síťové adaptéry, bezdrátové adaptéry, vytáčené linky atd.),
- *Důvěryhodná / lokální rozhraní* — rozhraní připojená k lokálním privátním sítím, které budou firewallem chráněny (typicky adaptéry *Ethernet* nebo *WiFi*),
- *Rozhraní pro VPN* — virtuální síťová rozhraní využívaná proprietárním řešením *Kerio VPN* (VPN server a vytvořené VPN tunely — podrobnosti viz kapitola 23),
- *Ostatní rozhraní* — rozhraní, která logicky nepatří do žádné z výše uvedených skupin (např. síťový adaptér pro DMZ, nevyužitá vytáčená linka atd.).

Skupiny rozhraní nelze vytvářet ani rušit (z hlediska konfigurace firewallu to nemá žádný smysl).

Při vytváření počáteční konfigurace firewallu prostřednictvím *Průvodce komunikačními pravidly* (viz kapitola 7.1) budou automaticky zařazena do správných skupin rozhraní vybraná pro připojení k Internetu a pro lokální síť. Zařazení rozhraní do skupin lze kdykoliv později upravit dle potřeby (s určitými omezeními — např. VPN server a VPN tunely patří vždy do skupiny *Rozhraní pro VPN*).

Přesun rozhraní do jiné skupiny se provádí přetažením myší nebo výběrem skupiny ve vlastnostech příslušného rozhraní — viz níže.

Poznámka: Pokud se neprovede počáteční konfigurace firewall pomocí průvodce, pak jsou všechna rozhraní (s výjimkou rozhraní pro VPN) zařazena do skupiny *Ostatní rozhraní*. Před vytvářením komunikačních pravidel doporučujeme správně definovat rozhraní pro připojení k Internetu a pro lokální síť — tím se značně zjednoduší definice vlastních pravidel.

Speciální rozhraní

V sekci *Rozhraní* se zobrazují také tato dvě speciální rozhraní:

VPN server
: Toto rozhraní představuje server pro připojení proprietárního VPN klienta (*Kerio VPN Client* — zdarma ke stažení na stránce `http://www.kerio.cz/cz/firewall/download`). VPN server je vždy zařazen do skupiny *Rozhraní pro VPN*.
Dvojitým kliknutím na toto rozhraní (případně stisknutím tlačítka *Změnit*) se otevírá dialog pro nastavení parametrů VPN serveru. Rozhraní *VPN server* nelze odstranit.
Podrobné informace o proprietárním VPN řešení *Kerio VPN* naleznete v kapitole 23.

Dial-In (pouze na systému Windows)
: Toto rozhraní představuje server služby *RAS* (telefonického připojení sítě) na počítači s *WinRoute*. S použitím rozhraní *Dial-In* lze definovat komunikační pravidla (viz kapitola 7) pro RAS klienty, kteří se na tento server připojují.

Rozhraní *Dial-In* je považováno za důvěryhodné (klient připojený přes toto rozhraní má přístup do lokální sítě). Toto rozhraní nelze konfigurovat ani odstranit. Pokud z nějakého důvodu RAS klienty nepovažujeme za součást důvěryhodné lokální sítě, můžeme rozhraní *Dial-In* přesunout do skupiny *Ostatní rozhraní*.
Poznámka:

1. Při použití RAS serveru společně s *WinRoute* je třeba nastavit RAS server tak, aby přidělovaly klientům IP adresy ze subsítě, která není použita v žádném segmentu lokální sítě. *WinRoute* provádí standardní IP směrování a při nedodržení uvedené podmínky nebude toto směrování fungovat správně.
2. Pro přidělování IP adres RAS klientům připojujícím se přímo k počítači s *WinRoute* *nelze* využít DHCP server ve *WinRoute*. Podrobnosti viz kapitola 8.2.

Zobrazení a změna parametrů rozhraní

WinRoute v seznamu rozhraní zobrazuje parametry, které souvisejí s konfigurací a činností firewallu:

Jméno
Jednoznačný název, který identifikuje rozhraní v rámci *WinRoute*. Zvolte jej tak, aby bylo zřejmé, o který adaptér se jedná (např. *Internet* pro rozhraní připojené k Internetu).
Název rozhraní může být kdykoliv později změněn (viz dále), aniž by tím došlo k ovlivnění funkce *WinRoute*.
Ikona vlevo od názvu zobrazuje typ rozhraní (síťový adaptér, vytáčené připojení, VPN server, VPN tunel).
Poznámka: Nebyl-li dosud název rozhraní zadán ručně, obsahuje tato položka jméno adaptéru z operačního systému (viz položka *Jméno adaptéru*).

IP adresa, Maska
IP adresa a maska subsítě přiřazené tomuto rozhraní.
Pokud má zvolený adaptér nastaveno více IP adres, zobrazuje se zde vždy primární IP adresa. V systému *Windows* je za primární adresu považována ta, která byla danému adaptéru přiřazena jako první.

Stav
Stav rozhraní (připojeno/odpojeno).

Internet
Indikace, jakým způsobem je rozhraní použito pro připojení k Internetu (primární/sekundární připojení, využitá šířka pásma při rozložení zátěže).

Podrobnosti
Identifikační řetězec adaptéru, který vrací příslušný ovladač zařízení.

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

Brána
IP adresa výchozí brány nastavené na příslušném rozhraní.

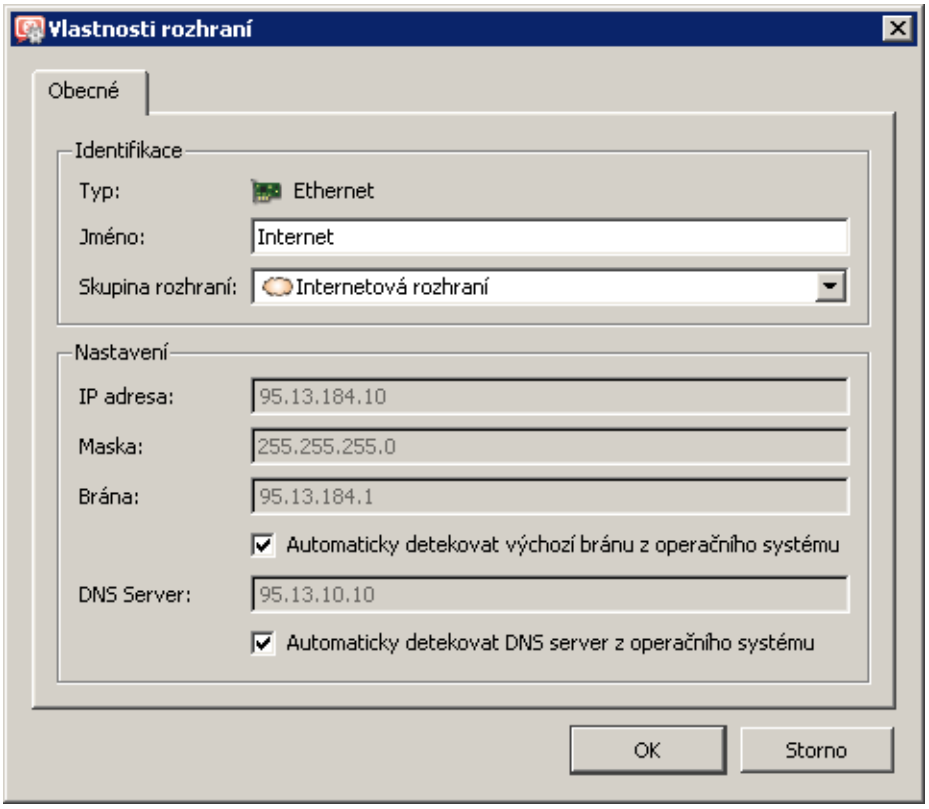
DNS
IP adresa primárního DNS serveru nastaveného na příslušném rozhraní.

MAC
Hardwarová (MAC) adresa příslušného síťového adaptéru. U vytáčených linek, rozhraní pro VPN atd. nemá tato položka smysl a je prázdná.

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 VPN tunel
Tímto tlačítkem lze vytvořit nový VPN tunel typu server-to-server. Podrobnosti o proprietárním VPN řešení *Kerio VPN* viz kapitola 23.
Poznámka: V *Software Appliance / VMware Virtual Appliance* je možné také přidávat nová rozhraní (vytáčené připojení, PPTP nebo PPPoE připojení) — viz sekce *Přidání nového rozhraní*. Je-li *WinRoute* nainstalován na systému *Windows*, pak je potřeba definovat nová připojení standardním způsobem přímo v operačním systému.

Změnit
Stisknutím tlačítka *Změnit* lze zobrazit podrobné informace a upravit parametry vybraného rozhraní.



Obrázek 5.2 Nastavení parametrů rozhraní

Každému rozhraní lze ve *WinRoute* přiřadit vlastní jméno (název rozhraní převzatý z operačního systému nemusí být vždy srozumitelný, dokonce ani jednoznačný). Dále lze změnit skupinu, do které je rozhraní zařazeno (Internet, chráněná lokální síť, jiná síť — např. DMZ).

Dále je možné změnit nastavení výchozí brány a DNS serverů. V edici *Software Appliance / VMware Virtual Appliance* je možné v tomto dialogu nastavit všechny parametry síťového rozhraní.

Jedná-li se o vytáčenou linku, umožňuje dialog nastavit také přihlašovací údaje a volby pro vytáčení (viz kapitola 6.2).

V případě rozhraní *VPN server* a VPN tunelů se zobrazí dialog pro nastavení parametrů VPN serveru (viz kapitola 23.1), resp. VPN tunelu (viz kapitola 23.3).

Odebrat

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

- jedná se o neaktivní (zakázaný) VPN tunel,
- jedná se o síťový adaptér, který již není v systému fyzicky přítomen nebo není aktivní,
- jedná se o vytáčenou linku, která již v systému neexistuje.

Síťový adaptér nebo vytáčenou linku definovanou v operačním systému či navázaný VPN tunel *WinRoute* nepovolí odebrat.

Poznámka:

1. Záznam o již neexistujícím síťovém adaptéru nebo odstraněné vytáčené lince nemá žádný vliv na činnost *WinRoute* — je považován za neaktivní, stejně jako vytáčená linka v zavěšeném stavu.
2. Při odstranění rozhraní se ve všech komunikačních pravidlech, ve kterých bylo toto rozhraní použito, dosadí do příslušné položky hodnota *Nic*. Všechna taková pravidla pak budou neaktivní. Tím je zajištěno, že odebrání rozhraní nijak neovlivní smysl komunikačních pravidel (podrobnosti viz kapitola 7.3).

Vytočit, Zavěsit / Povolit, Zakázat

Funkce těchto tlačítek závisí na typu vybraného rozhraní:

- V případě vytáčené linky, PPTP nebo PPPoE připojení jsou tlačítka označena *Vytočit* a *Zavěsit* a slouží k ručnímu ovládání vybrané linky.
  Poznámka: Uživatelé s příslušným právem mohou rovněž ovládat vytáčené linky v uživatelském WWW rozhraní (viz kapitola 15.2 a manuál *Kerio WinRoute Firewall — Příručka uživatele*).
- V případě VPN tunelu jsou tato tlačítka označena *Povolit* a *Zakázat* a slouží k aktivaci / deaktivaci vybraného VPN tunelu (podrobnosti viz kapitola 23.3).
  V edici *Software Appliance / VMware Virtual Appliance* lze povolit nebo zakázat také jednotlivé síťové adaptéry.
- Je-li vybráno rozhraní *Dial-in* nebo VPN server, jsou tato tlačítka neaktivní.

Přidání nového rozhraní (Software Appliance / VMware Virtual Appliance)

WinRoute v edici *Software Appliance / VMware Virtual Appliance* umožňuje přidávat nová síťová rozhraní (vytáčené linky, PPPoE a PPTP připojení) přímo v administrační konzoli.

Stisknutím tlačítka *Přidat* se zobrazí nabídka, ze které vybereme požadovaný typ nového rozhraní (vytáčenou linku lze přidat pouze v případě, že je v počítači s firewallem nainstalován analogový nebo ISDN modem).

Novému rozhraní je potřeba přiřadit dostatečně popisné jméno, pod kterým bude rozhraní zobrazováno ve *WinRoute*, a zařadit jej do některé skupiny rozhraní (skupinu lze samozřejmě kdykoliv později změnit dle potřeby).

Další parametry rozhraní závisejí na zvoleném typu rozhraní. Ve většině případů je potřeba zadat také uživatelské jméno a heslo pro ověření přístupu.

Volitelně lze zadat IP adresu specifického DNS serveru, který bude použit jako primární DNS server při přístupu do Internetu přes toto rozhraní.

Záložka *Nastavení vytáčení* umožňuje nastavit časové intervaly, ve kterých má být připojení trvale navázáno nebo trvale odpojeno. Mimo tyto intervaly bude připojení navazováno na žádost (tzn. bude automaticky navázáno vždy, pokud *WinRoute* potřebuje odeslat paket do příslušné sítě). Podrobné informace o linkách vytáčených na žádost naleznete v kapitole 6.2 a 25.5.

Kapitola 6

Internetové připojení

Základní funkcí *WinRoute* je připojení lokální sítě k Internetu prostřednictvím jednoho nebo více internetových připojení (internetových linek). V závislosti na počtu a typu linek nabízí *WinRoute* různé možnosti připojení k Internetu:

Jedna linka — trvalé připojení
: Nejběžnější způsob připojení lokální sítě k Internetu. K dispozici je pouze jedno internetové připojení, které má trvalý charakter (typicky *Ethernet*, *WiFi*, *ADSL* nebo kabelový modem). Lze použít i linky, které mají charakter vytáčeného připojení, ale mohou být trvale připojeny — např. připojení *PPPoE* nebo *CDMA* modem.

Jedna linka — vytáčení na žádost
: Tento způsob připojení je vhodný pro linky, které jsou účtovány podle doby připojení — typicky modem pro analogovou nebo *ISDN* linku. Linka je ve výchozím stavu zavěšena a *WinRoute* ji automaticky vytočí v okamžiku, kdy zaznamená požadavek na přístup z lokální sítě do Internetu. Pokud nejsou po lince přenášena žádná data, *WinRoute* ji po nastavené době opět zavěsí, čímž snižuje náklady na připojení.

Dvě linky — zálohování připojení
: Pokud je kladen důraz na spolehlivost internetového připojení (dostupnost Internetu) a jsou k dispozici dvě internetové linky, pak lze využít funkci zálohování internetového připojení. V případě výpadku primární linky začne *WinRoute* automaticky používat záložní linku (pevnou nebo vytáčenou). Uživatelé tak zaznamenají jen velmi krátkodobý výpadek internetového připojení. Po obnovení funkčnosti primární linky *WinRoute* automaticky přepne internetové připojení zpět na primární linku. Při přepnutí zpět již většina uživatelů ani nezaznamená výpadek.

Dvě a více linek — rozložení zátěže
: Je-li nejdůležitějším kritériem propustnost (rychlost) internetového připojení, pak může *WinRoute* použít více internetových linek zároveň a rozdělit data přenášená mezi lokální sítí a Internetem mezi tyto linky. Při standardním nastavení se zároveň jedná o zálohované připojení — při výpadku některé z linek budou data automaticky rozložena mezi zbývající linky.

Ve všech případech *WinRoute* pracuje v režimu sdílení internetového připojení. Pro sdílení připojení se využívá technologie překladu IP adres (NAT), kdy je celá lokální síť skryta za veřejnou IP adresou firewallu (resp. několika veřejnými adresami — dle použitého způsobu internetového připojení). *WinRoute* lze rovněž použít jako neutrální směrovač (tj. směrovač bez překladu IP adres). Tento režim však není příliš vhodný pro připojení lokální sítě k Internetu — vyžaduje pokročilejší nastavení směrování a zabezpečení.

Při konfiguraci internetového připojení ve *WinRoute* je nejprve potřeba v sekci *Konfigurace → Rozhraní* vybrat požadovaný způsob připojení k Internetu, nastavit příslušná rozhraní pro připojení k Internetu a definovat odpovídající komunikační pravidla (viz kapitola 7.3).

Tip

Všechna potřebná nastavení mohou být provedena automaticky pomocí *Průvodce komunikačními pravidly* — viz kapitola 7.1. V následujících kapitolách bude uvedeno nastavení daného typu internetového připojení pomocí průvodce a popis odpovídající konfigurace rozhraní a komunikačních pravidel. Tyto informace lze využít pro úpravu nastavení dle potřeby (např. při připojení nové lokální subsítě nebo změně internetového připojení).

6.1 Trvalé připojení jednou linkou

Požadavky

Počítač s *WinRoute* musí být připojen k Internetu pevnou linkou (typicky adaptér *Ethernet* nebo *WiFi*). Parametry toho rozhraní budou nastaveny podle údajů od poskytovatele internetového připojení nebo mohou být konfigurovány automaticky protokolem DHCP.

Alternativně je možné použít linku, která má charakter vytáčeného připojení, ale může být trvale připojena — např. připojení *PPPoE* nebo *CDMA* modem. Linku tohoto typu bude *WinRoute* udržovat trvale připojenou (při výpadku dojde ihned k automatickému obnovení připojení).

Dále musí být přítomen jeden nebo více síťových adaptérů pro připojení segmentů lokální sítě. Na žádném z těchto adaptérů *nesmí* být nastavena výchozí brána!

Je-li to možné, doporučujeme vyzkoušet funkčnost internetového připojení ještě před instalací *WinRoute*.

Konfigurace pomocí průvodce

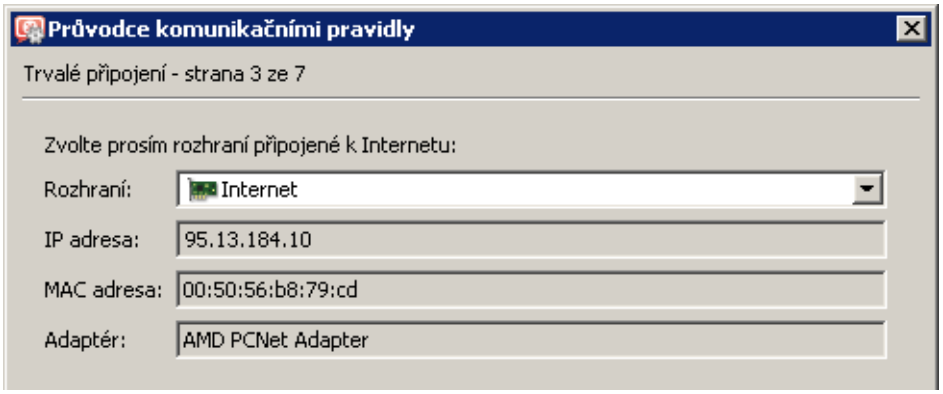
V *Průvodci komunikačními pravidly* (viz kapitola 7.1) ve druhém kroku zvolíme možnost *Jedna internetová linka — trvalé připojení*.

Ve třetím kroku průvodce pak vybereme odpovídající síťové rozhraní (internetovou linku). *WinRoute* automaticky nabídne rozhraní, na kterém detekoval výchozí bránu. Proto je ve většině případů v tomto kroku již přednastaven správný adaptér.

Pokud vybereme linku, která je definována jako vytáčené připojení (viz výše), pak je potřeba také zadat příslušné uživatelské jméno a heslo. Pokud jsou tyto údaje v operačním systému uloženy, může je *WinRoute* načíst automaticky.

V edici *Software Appliance / VMware Virtual Appliance* je přímo v průvodci možné:

Obrázek 6.1 Průvodce komunikačními pravidly — trvalé připojení jednou linkou



Obrázek 6.2 Průvodce komunikačními pravidly — výběr rozhraní pro připojení k Internetu

- Konfigurovat parametry vybraného rozhraní,
- Vytvořit nové rozhraní (*PPPoE*, *PPTP* nebo vytáčené připojení).

Podrobné informace o síťových rozhraních naleznete v kapitole 5.

Poznámky:

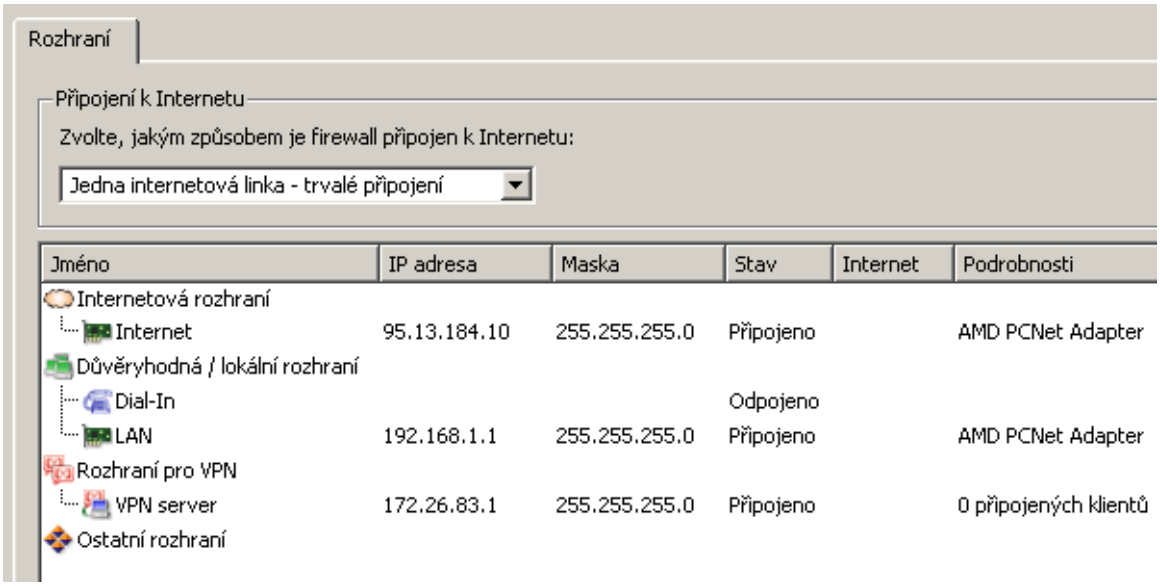
1. Na prvním místě seznamu je nabízeno internetové rozhraní, na němž je nastavena výchozí brána. Proto je ve většině případů v tomto kroku již přednastaven správný adaptér.

2. Pokud má zvolený adaptér nastaveno více IP adres, zobrazuje se zde vždy primární IP adresa. V systému *Windows* je za primární adresu považována ta, která byla danému adaptéru přiřazena jako první.

3. Zbývající kroky *Průvodce komunikačními pravidly* již nesouvisejí s typem internetového připojení. Tyto kroky jsou popsány samostatně v kapitole 7.1

Výsledná konfigurace rozhraní

Po dokončení *Průvodce komunikačními pravidly* si můžeme v sekci *Konfigurace* → *Rozhraní* prohlédnout výslednou konfiguraci rozhraní a v případě potřeby ji dále upravit.



Obrázek 6.3 Konfigurace rozhraní — připojení jednou pevnou linkou

Do skupiny *Internetová rozhraní* je zařazen pouze adaptér *Internet* vybraný ve třetím kroku průvodce. Ostatní rozhraní (včetně rozhraní *Dial-In*) jsou považována za segmenty lokální sítě a jsou zařazena do skupiny *Důvěryhodná / lokální rozhraní*.

Pokud nastavení rozhraní neodpovídá skutečné konfiguraci sítě (např. některý adaptér je určen pro DMZ), můžeme přesunout příslušné rozhraní do skupiny *Ostatní rozhraní*. Pro tato rozhraní je pak nutné ručně definovat odpovídající komunikační pravidla (viz kapitola 7.3).

Do skupiny *Internetová rozhraní* je rovněž možné přidat další rozhraní. Pakety pak budou směrovány do příslušných cílových sítí dle systémové směrovací tabulky (viz též kapitola 18.1) a bude prováděn překlad IP adres (NAT). V praxi však takováto konfigurace nemá příliš velký význam.

Upozornění

V režimu *Jedna internetová linka* musí být nastavena výchozí brána pouze na „hlavním“ internetovém rozhraní! Pokud *WinRoute* detekuje více výchozích bran, zobrazí se chybové hlášení. Tento problém je potřeba ihned vyřešit, jinak nebude komunikace z firewallu a lokální sítě do Internetu fungovat správně.

6.2 Připojení jednou vytáčenou linkou - vytáčení na žádost

Je-li počítač s *WinRoute* připojen k 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).
- Udržování linky trvale připojené nebo trvale zavěšené ve zvolených časových intervalech.

Požadavky

V počítači s *WinRoute* musí být nainstalováno příslušné zařízení (zpravidla analogový modem nebo ISDN modem) a v operačním systému vytvořeno odpovídající vytáčené připojení. U vytáčeného připojení nemusejí být uloženy přihlašovací údaje (je-li k tomu nějaký důvod), tyto údaje lze zadat přímo ve *WinRoute*. Dále musí být přítomen jeden nebo více síťových adaptérů pro připojení segmentů lokální sítě. Na žádném z těchto adaptérů *nesmí* být nastavena výchozí brána!

Doporučujeme vytvořit vytáčené připojení a prověřit jeho funkčnost ještě před instalací *WinRoute*.

Upozornění

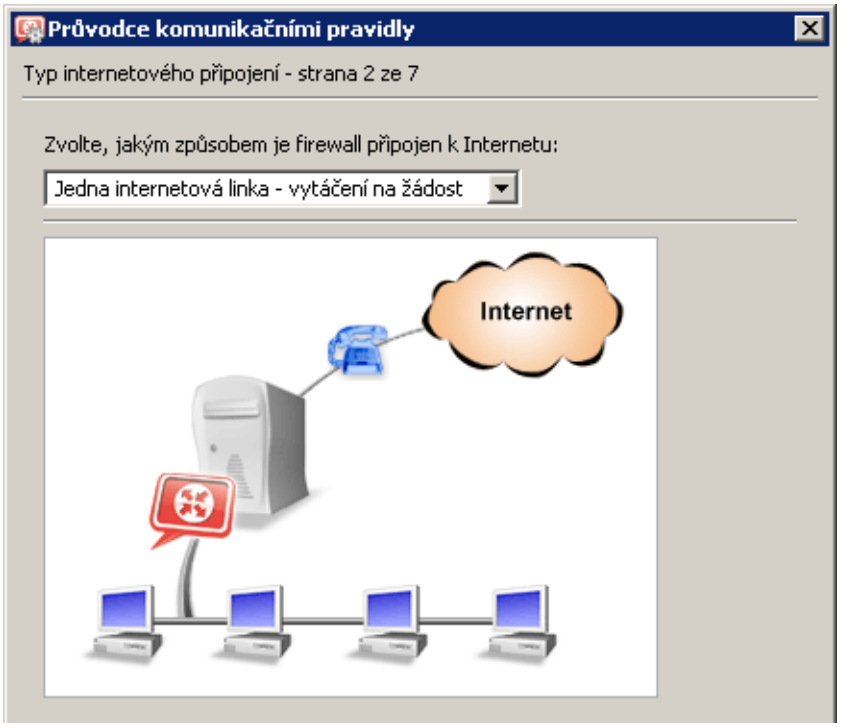
Před konfigurací lokální sítě a firewallu s použitím internetové linky vytáčené na žádost doporučujeme důkladně prostudovat informace uvedené v kapitole 25.5. Vhodným návrhem konfigurace sítě s ohledem na specifické vlastnosti linky vytáčené na žádost lze předejít mnoha pozdějším problémům.

Konfigurace pomocí průvodce

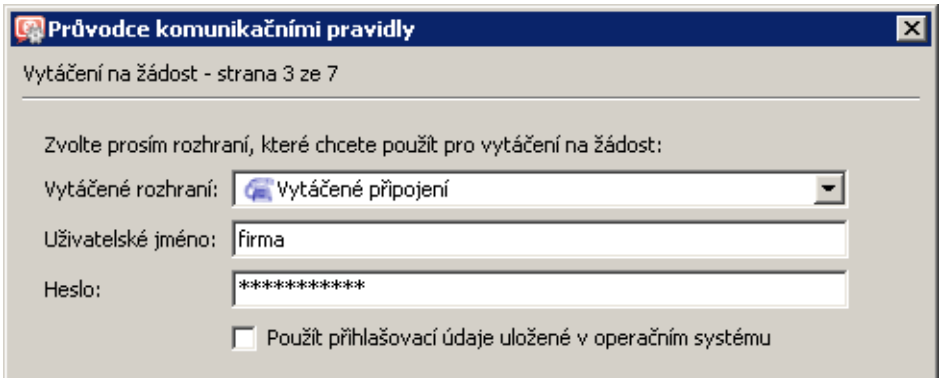
V *Průvodci komunikačními pravidly* (viz kapitola 7.1) ve druhém kroku zvolíme možnost *Jedna internetová linka — vytáčení na žádost*.

Ve třetím kroku průvodce pak vybereme odpovídající vytáčené připojení (internetovou linku). Pokud nejsou v operačním systému uloženy přihlašovací údaje, pak je potřeba také zadat příslušné uživatelské jméno a heslo.

V edici *Software Appliance / VMware Virtual Appliance* je přímo v průvodci možné:



Obrázek 6.4 Průvodce komunikačními pravidly — vytáčení linky na žádost



Obrázek 6.5 Průvodce komunikačními pravidly — výběr rozhraní pro připojení k Internetu

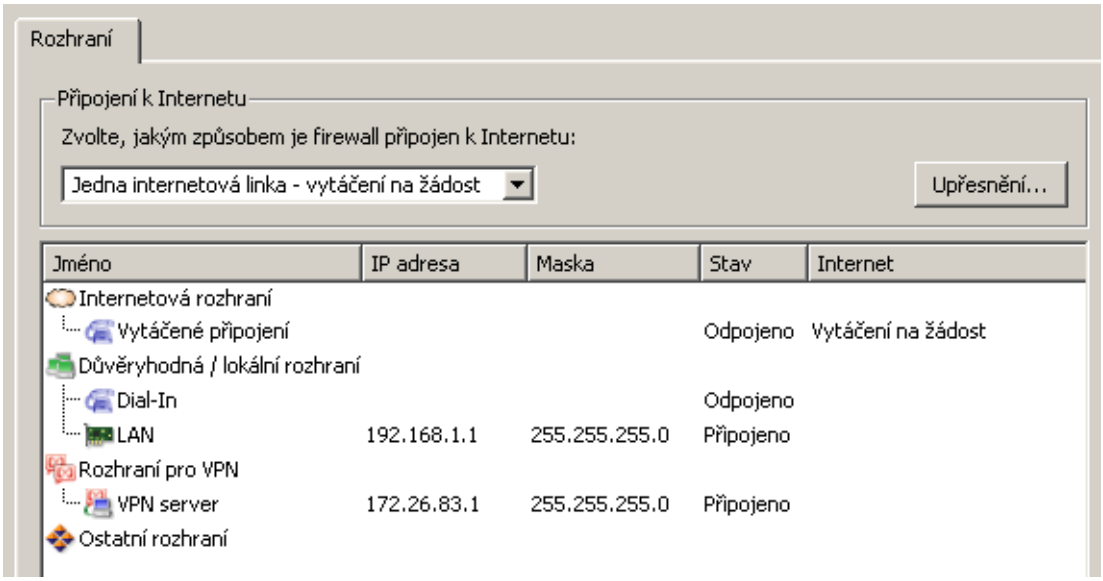
- Konfigurovat parametry vybraného rozhraní,
- Vytvořit nové rozhraní (*PPPoE*, *PPTP* nebo vytáčené připojení).

Podrobné informace o síťových rozhraních naleznete v kapitole 5.

Výsledná konfigurace rozhraní

Po dokončení *Průvodce komunikačními pravidly* si můžeme v sekci *Konfigurace* → *Rozhraní* prohlédnout výslednou konfiguraci rozhraní a v případě potřeby ji dále upravit.

Do skupiny *Internetová rozhraní* je zařazena pouze linka *Vytáčené připojení* vybraná ve třetím kroku průvodce. Toto připojení je automaticky označeno jako linka vytáčená na žádost (viz informace ve sloupci *Internet*). Ostatní rozhraní (včetně rozhraní *Dial-In*) jsou považována za segmenty lokální sítě a jsou zařazena do skupiny *Důvěryhodná / lokální rozhraní*.



Obrázek 6.6 Konfigurace rozhraní — linka vytáčená na žádost

Ve skupině *Internetová rozhraní* může být zařazeno více vytáčených linek. Pro vytáčení na žádost však může být nastavena vždy pouze jedna linka. Pokud dojde k ručnímu vytočení některé další linky, pak bude *WinRoute* směrovat pakety do příslušné cílové sítě dle systémové směrovací tabulky (viz též kapitola 18.1) a provádět překlad IP adres (NAT). Takováto konfigurace však nemá téměř žádný praktický význam. Do skupiny *Internetová rozhraní* proto doporučujeme zařadit vždy pouze jednu linku, která bude vytáčena na žádost.

Chceme-li změnit linku, která má být vytáčena na žádost, použijeme volbu v dialogu pro změnu parametrů rozhraní (viz kapitola 5) nebo v kontextovém menu (po kliknutí pravým tlačítkem myši na vybranou linku).

Upozornění

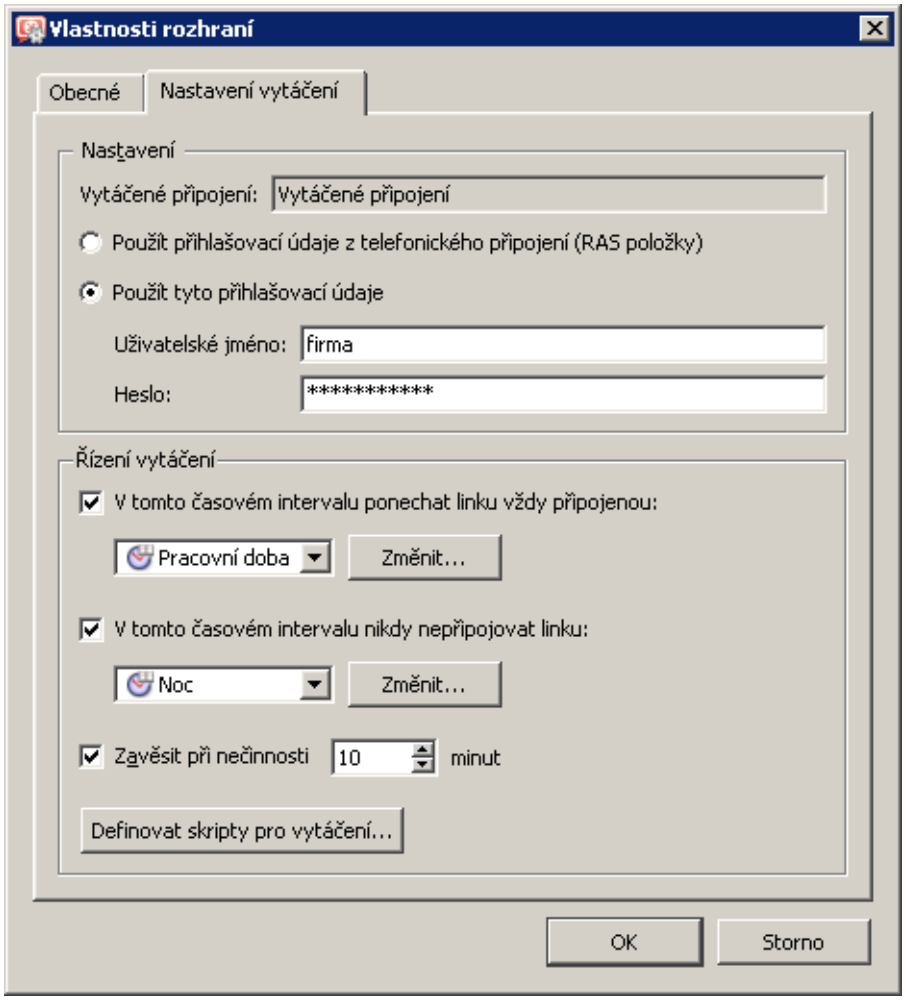
V režimu *Vytáčení na žádost* nesmí být na žádném síťovém rozhraní firewallu nastavena výchozí brána! Vytáčení na žádost funguje na základě neexistence výchozí brány (pokud ve směrovací tabulce neexistuje cesta, kam by měl být paket směrován, pak *WinRoute* vytvoří výchozí cestu vytočením internetové linky).

Volby pro vytáčení linky

Pro vytáčené linky je dialog pro nastavení parametrů rozhraní (viz kapitola 5) rozšířen o záložku *Nastavení vytáčení*, která umožňuje nastavit specifické parametry pro vytáčená připojení:

Přihlašovací údaje

Dojde-li ke změně přihlašovacích údajů k příslušnému vytáčenému připojení, můžeme je zde aktualizovat, případně použít údaje uložené v operačním systému (pokud byly mezitím v systému uloženy).



Obrázek 6.7 Vlastnosti rozhraní — nastavení vytáčení

Časové intervaly pro trvalé připojení a trvalé zavěšení

V některých případech může být požadováno, aby vytáčení na žádost fungovalo jen v určitém čase (typicky v pracovní době) a mimo tuto dobu zůstala linka zavěšená. S ohledem na tarif telefonního operátora může být v době s velkou intenzitou síťového provozu naopak výhodnější ponechat linku trvale vytočenou.

Pro tyto účely je možné nastavit časové intervaly, kdy má být linka trvale připojena a kdy naopak trvale zavěšena.

Pokud se vybrané časové intervaly překrývají, pak má vyšší prioritu interval, ve kterém je linka trvale zavěšena. V časech mimo nastavené intervaly je linka vytáčena na žádost.

Poznámka:

1. Pokud je ve směrovací tabulce ve *WinRoute* definována statická cesta přes vytáčenou linku, pak tato linka bude vytočena vždy, když bude touto cestou směrován nějaký paket. Nastavení intervalu, kdy má být linka trvale zavěšena, bude v tomto případě ignorováno.

Podrobnosti viz kapitola 18.1.

2. Konfigurace vytáčení neobsahuje explicitní volbu pro obnovení připojení po výpadku. V případě výpadku připojení bude nebo nebude obnoveno v závislosti na režimu linky v aktuálním okamžiku:
   - Pokud má být linka trvale připojena, pak bude spojení automaticky ihned obnoveno.
   - Má-li být linka trvale zavěšena, pak připojení obnoveno nebude.
   - V režimu vytáčení na žádost (tj. mimo zde nastavené intervaly) bude připojení obnoveno s prvním následujícím požadavkem (paketem z lokální sítě do Internetu).

Automatické zavěšení linky při nečinnosti

Vytáčené linky jsou zpravidla účtovány podle doby připojení. Pokud připojením nejsou přenášena žádná data, je zbytečné, aby linka zůstávala připojená. Proto je možné nastavit dobu, po které bude linka automaticky zavěšena.

Pro optimální nastavení doby nečinnosti je třeba vzít v úvahu způsob, jakým je připojení účtováno. Příliš krátká doba způsobí časté zavěšování a vytáčení linky, což může náklady naopak zvýšit (a navíc zhoršit uživatelský komfort).

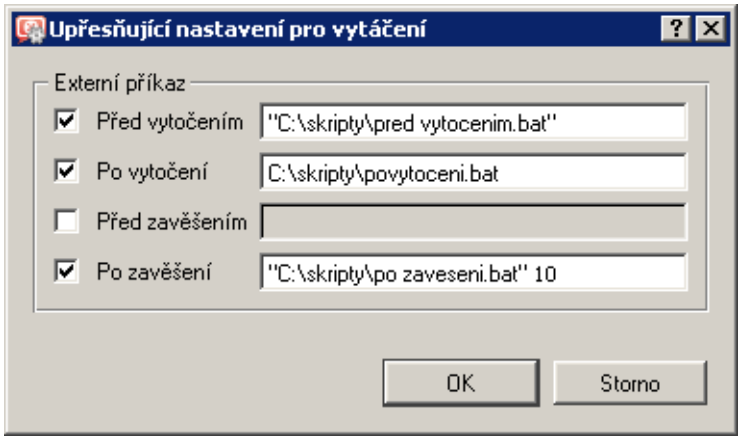
Poznámka: V časovém intervalu, kdy má být linka trvale připojena (viz výše), je doba nečinnosti ignorována.

Skripty pro vytáčení

V některých případech vzniká potřeba spustit při vytáčení nebo zavěšování linky určitý program nebo skript (dávkový příkaz). Může se jednat např. o speciální typ modemu, který musí být ovládán programem dodaným jeho výrobcem.

WinRoute umožňuje spustit libovolný program nebo příkaz v těchto okamžicích: *Před vytočením* linky, *Po vytočení* linky, *Před zavěšením* linky a *Po zavěšení* linky.

Poznámka: V případě akcí *Před vytočením* a *Před zavěšením* se po spuštění programu nečeká na jeho ukončení.



Obrázek 6.8 Vytáčená linka — externí příkazy

Cesta ke spustitelnému souboru musí být vždy kompletní. Pokud cesta obsahuje mezeru, musí být vložena do uvozovek, jinak bude část za mezerou považována za parametr(y) dávkového souboru. Je-li cesta k souboru v uvozovkách, pak je případný text za uzavírajícími uvozovkami rovněž považován za parametr(y) dávkového souboru.

Upozornění

WinRoute běží v operačním systému jako služba, a proto budou zadané externí aplikace nebo příkazy operačního systému spouštěny pouze na pozadí (pod účtem *SYSTEM*). Totéž platí pro všechny příkazy a externí programy volané v zadaných skriptech. Z tohoto důvodu není vhodné pro výše popsané akce používat interaktivní aplikace (tzn. aplikace, které vyžadují zásah uživatele). Interaktivní aplikace by zůstala „neviditelně“ spuštěná až do restartu systému nebo ukončení příslušného procesu pomocí *Správce úloh systému Windows*. V některých případech by taková aplikace mohla zároveň blokovat další vytočení nebo zavěšení linky.

6.3 Zálohované internetové připojení

WinRoute umožňuje zálohovat internetové připojení další linkou. Záložní připojení se automaticky aktivuje, jestliže je detekován výpadek primárního připojení. Jakmile *WinRoute* zjistí, že je primární připojení opět funkční, automaticky deaktivuje záložní připojení a začne opět používat primární připojení.

Požadavky

Počítač s *WinRoute* musí mít dvě síťová rozhraní pro připojení k Internetu: pevnou linku (*Ethernet*, *WiFi*) nebo trvale připojenou vytáčenou linku (*CDMA*, *PPPoE*) pro primární připojení a pevnou nebo vytáčenou linku pro sekundární (záložní) připojení.

Dále musí být přítomen jeden nebo více síťových adaptérů pro připojení segmentů lokální sítě. Na žádném z adaptérů pro lokální síť *nesmí* být nastavena výchozí brána!

V případě vytáčených linek je potřeba v operačním systému také definovat odpovídající telefonické připojení. Přihlašovací údaje k telefonickým připojením nemusejí být v systému uloženy (je-li k tomu nějaký důvod), tyto údaje lze zadat přímo ve *WinRoute*.

Primární i záložní linka mohou být konfigurovány automaticky protokolem DHCP. *WinRoute* pak detekuje z operačního systému všechny potřebné parametry.

Doporučujeme prověřit funkčnost primární a sekundární linky ještě před instalací *WinRoute*:

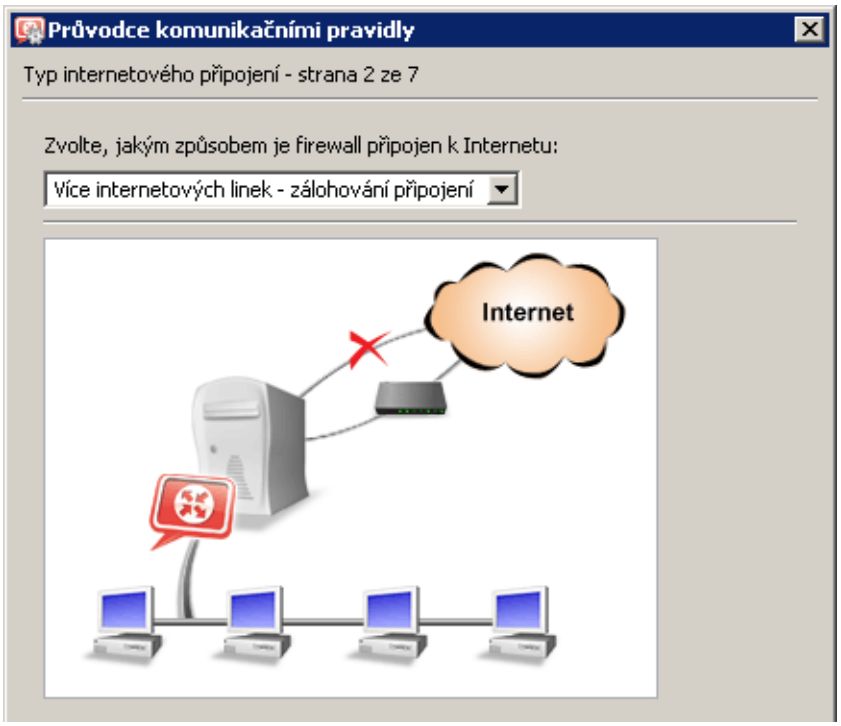
- Pokud se jedná o dvě vytáčené linky, vytočíme postupně každou z nich a prověříme přístup do Internetu.
- Je-li primární linka pevná a záložní linka vytáčená, otestujeme nejprve připojení primární linkou a poté vytočíme záložní linku. Po vytočení linky vznikne nová výchozí cesta přes tuto linku, a tak můžeme otestovat přístup do Internetu přes záložní linku.
- V případě dvou pevných linek je nejjednodušší zakázat v operačním systému jedno připojení a vyzkoušet přístup do Internetu přes druhou (povolenou) linku. Tento postup pak zopakujeme pro první linku.

Upozornění

Zálohování internetového připojení je vhodné pouze pro trvalé připojení (tzn. primární připojení je realizováno síťovým adaptérem nebo trvale připojenou vytáčenou linkou). V opačném případě by docházelo k automatické aktivaci záložního připojení při každém zavěšení primární linky.

Konfigurace pomocí průvodce

V *Průvodci komunikačními pravidly* (viz kapitola 7.1) ve druhém kroku zvolíme možnost *Více internetových linek — zálohování připojení.*



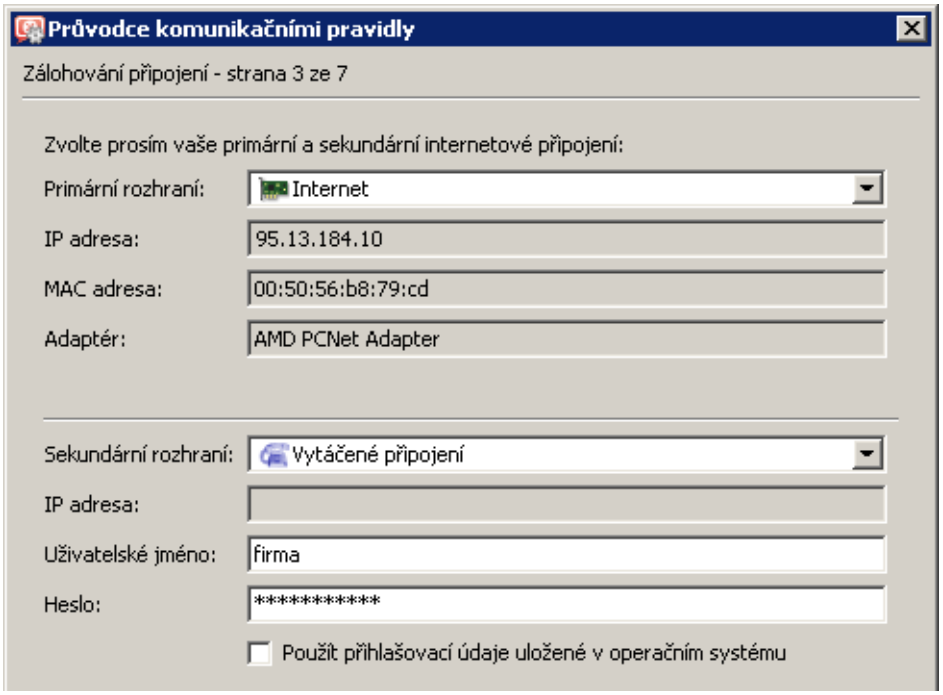
Obrázek 6.9 Průvodce komunikačními pravidly — zálohované internetové připojení

Ve třetím kroku průvodce pak vybereme síťové rozhraní pro primární připojení (pevnou nebo trvale připojenou vytáčenou linku) a pro sekundární připojení (pevnou nebo vytáčenou linku). Pokud u vybraných telefonických připojení nejsou v operačním systému uloženy přihlašovací údaje, zadáme příslušné jméno a heslo.

V edici *Software Appliance / VMware Virtual Appliance* je přímo v průvodci možné:

- Konfigurovat parametry vybraného primárního a sekundárního rozhraní,
- Vytvořit nové primární a/nebo sekundární rozhraní (*PPPoE*, *PPTP* nebo vytáčené připojení).

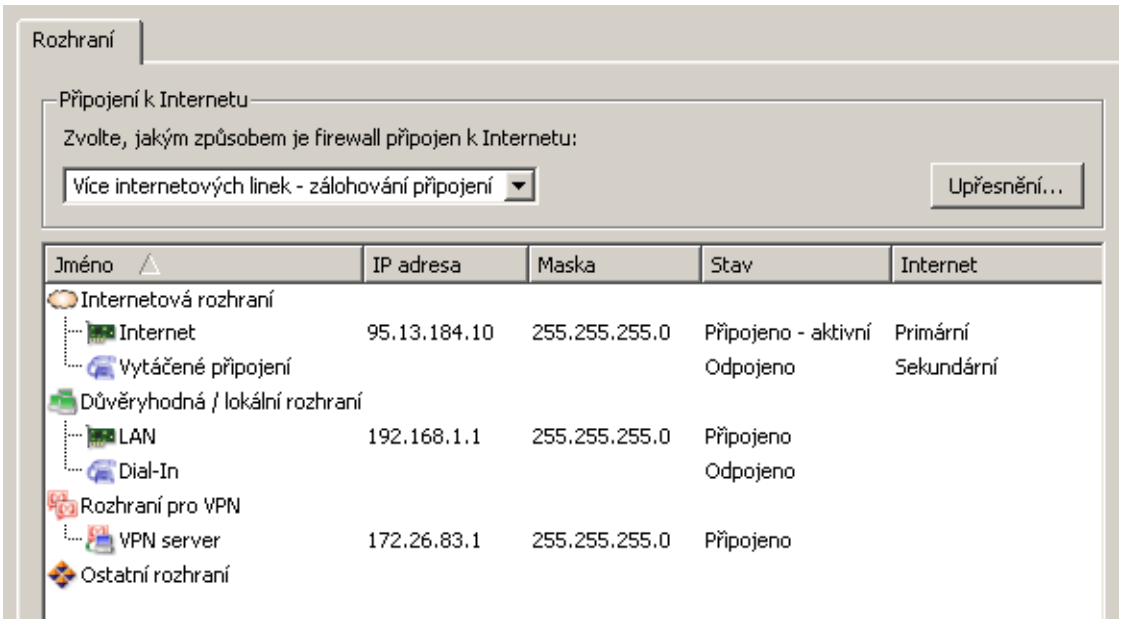
Podrobné informace o síťových rozhraních naleznete v kapitole 5.



Obrázek 6.10 Průvodce komunikačními pravidly — zálohování pevné linky vytáčeným připojením

Výsledná konfigurace rozhraní

Po dokončení *Průvodce komunikačními pravidly* si můžeme v sekci *Konfigurace* → *Rozhraní* prohlédnout výslednou konfiguraci rozhraní a v případě potřeby ji dále upravit.



Obrázek 6.11 Konfigurace rozhraní — zálohované internetové připojení

Do skupiny *Internetová rozhraní* jsou zařazeny linky *Internet* a *Vytáčené připojení* vybrané ve třetím kroku průvodce jako primární a sekundární (záložní) internetové připojení. Ve sloupci *Internet* je zobrazeno, která linka je použita jako primární a která jako sekundární připojení. Ve sloupci *Stav* je kromě stavu linky samotné (připojena/odpojena) zobrazována také informace, zda je linka aktivní — tzn. zda je právě použita jako internetové připojení.

Ostatní rozhraní (včetně rozhraní *Dial-In*) jsou považována za segmenty lokální sítě a jsou zařazena do skupiny *Důvěryhodná / lokální rozhraní*.

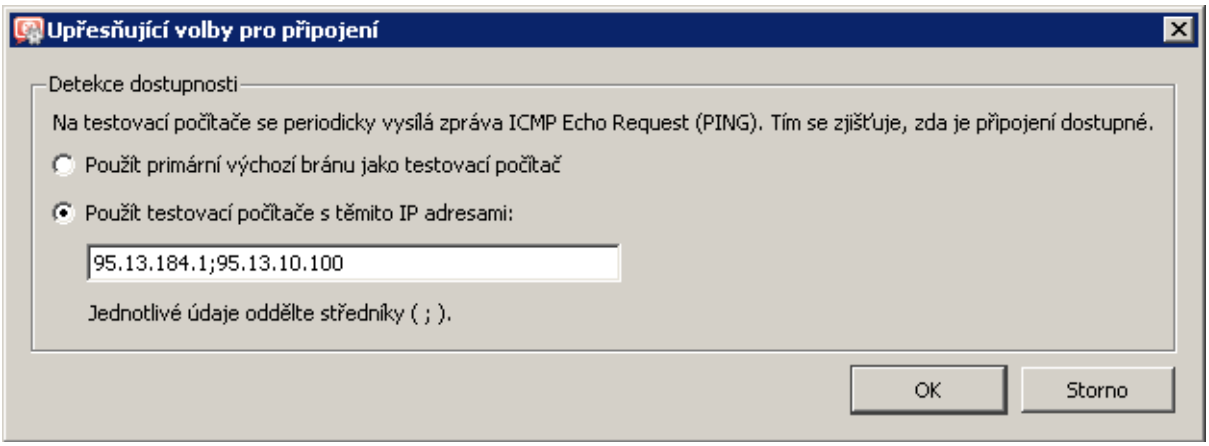
Ve skupině *Internetová rozhraní* mohou být zařazeny i další linky. Pokud budou tyto linky připojené, bude probíhat standardní směrování s překladem IP adres (NAT). Je zřejmé, že tyto linky nebudou zálohovány. Takováto konfigurace nemá příliš velký praktický význam. Doporučujeme do skupiny *Internetová rozhraní* zařadit pouze linky pro primární a sekundární internetové připojení.

Chceme-li změnit nastavení primárního a sekundárního připojení, použijeme volby v dialogu pro změnu parametrů rozhraní (viz kapitola 5) nebo v kontextovém menu (po kliknutí pravým tlačítkem myši na vybranou linku). Vždy však může být pouze jedna linka nastavena jako primární připojení a pouze jedna linka jako sekundární připojení.

Testovací počítače

Funkčnost primárního internetového připojení se ověřuje periodickým vysíláním *ICMP* žádostí o odezvu (*PING*) na určité počítače nebo síťová zařízení. Standardně se jako testovací počítač používá výchozí brána primárního připojení. Je zřejmé, že pokud není výchozí brána dostupná, není toto internetové připojení (plně) funkční.

Pokud z nějakého důvodu nelze použít jako testovací počítač primární výchozí bránu, můžeme po stisknutí tlačítka *Upřesnění* specifikovat IP adresy jednoho nebo více testovacích počítačů. Je-li alespoň jeden z testovacích počítačů dostupný, považuje se primární internetové připojení za funkční.



Obrázek 6.12 Zálohování internetového připojení — nastavení testovacích počítačů

Poznámka:

1. Testovací počítač nesmí blokovat zprávy *ICMP Echo Request* (*PING*), které *WinRoute* používá pro testování jeho dostupnosti — jinak by byl vždy vyhodnocen jako nedostupný. Toto je typický případ, kdy nelze použít primární výchozí bránu jako testovací počítač.

2. Jako testovací počítače je třeba použít počítače nebo síťová zařízení, která jsou trvale v provozu (např. servery, směrovače apod.). Použít jako testovací počítač pracovní stanici, která je v provozu několik hodin denně, nemá příliš velký smysl.

3. *ICMP* zprávy odesílané na testovací počítače nelze zablokovat komunikačními pravidly firewallu.

6.4 Rozložení zátěže internetového připojení

Jsou-li k dispozici alespoň dvě internetové linky, může *WinRoute* část internetové komunikace posílat přes jednu linku a část přes jinou linku. Výhody jsou zřejmé — zvýší se propustnost internetového připojení (rychlost přenosu dat mezi lokální sítí a Internetem) a zkrátí se doba odezvy při přístupu k serverům v Internetu. Pokud nejsou definována speciální komunikační pravidla (tzv. *policy routing* — viz kapitola 7.5), pak jsou jednotlivé linky navíc vzájemně zálohovány (viz též kapitola 6.3) — při výpadku některé linky bude komunikace směrována přes jinou linku.

Poznámka:

1. Rozložení zátěže sítě je aplikováno pouze na komunikaci směrovanou výchozí cestou do Internetu. Pokud je ve směrovací tabulce (viz kapitola 18.1) definována cesta do určité cílové sítě, pak bude komunikace do této sítě vždy směrována přes příslušné rozhraní.

2. Rozložení zátěže se neaplikuje na komunikaci samotného firewallu. Tato komunikace je zpracovávána přímo operačním systémem, a proto zde probíhá standardní směrování (bude vždy použita výchozí cesta s nejnižší metrikou).

Požadavky

Počítač s *WinRoute* musí mít dvě síťová rozhraní pro připojení k Internetu, a to pevné linky (*Ethernet*, *WiFi*) nebo trvale připojené vytáčené linky (*CDMA*, *PPPoE*). Klasické vytáčené linky (analogový modem, *ISDN*) nejsou vhodné, protože v režimu rozložení zátěže internetového připojení nelze vytáčet linku na žádost.

Dále musí být přítomen jeden nebo více síťových adaptérů pro připojení segmentů lokální sítě. Na žádném z adaptérů pro lokální síť *nesmí* být nastavena výchozí brána!

V případě linek vytáčeného charakteru (*CDMA*, *PPPoE*) je potřeba v operačním systému také definovat odpovídající telefonické připojení. Přihlašovací údaje k telefonickým připojením nemusejí být v systému uloženy (je-li k tomu nějaký důvod), tyto údaje lze zadat přímo ve *WinRoute*.

Primární i záložní linka mohou být konfigurovány automaticky protokolem DHCP. *WinRoute* pak detekuje z operačního systému všechny potřebné parametry.

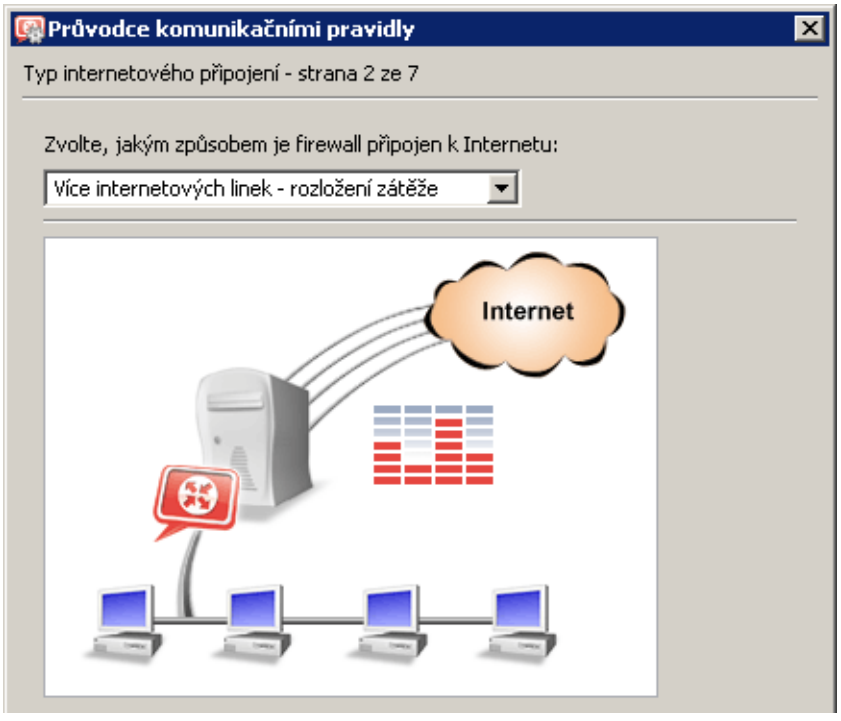
Doporučujeme prověřit funkčnost jednotlivých internetových linek ještě před instalací *WinRoute*. Možné způsoby testování (pro dvě linky):

- Pokud se jedná o dvě linky vytáčeného charakteru, připojíme postupně každou z nich a prověříme přístup do Internetu.
- Je-li jedna linka pevná a druhá linka vytáčená, otestujeme nejprve připojení pevnou linkou a poté vytočíme druhou linku. Po vytočení linky vznikne nová výchozí cesta přes tuto linku, a tak můžeme otestovat přístup do Internetu přes záložní linku.
- V případě dvou pevných linek je nejjednodušší zakázat v operačním systému jedno připojení a vyzkoušet přístup do Internetu přes druhou (povolenou) linku. Tento postup pak zopakujeme pro první linku.

Obdobně lze postupovat pro libovolný počet internetových linek.

Konfigurace pomocí průvodce

V *Průvodci komunikačními pravidly* (viz kapitola 7.1) ve druhém kroku zvolíme možnost *Více internetových linek — rozložení zátěže*.



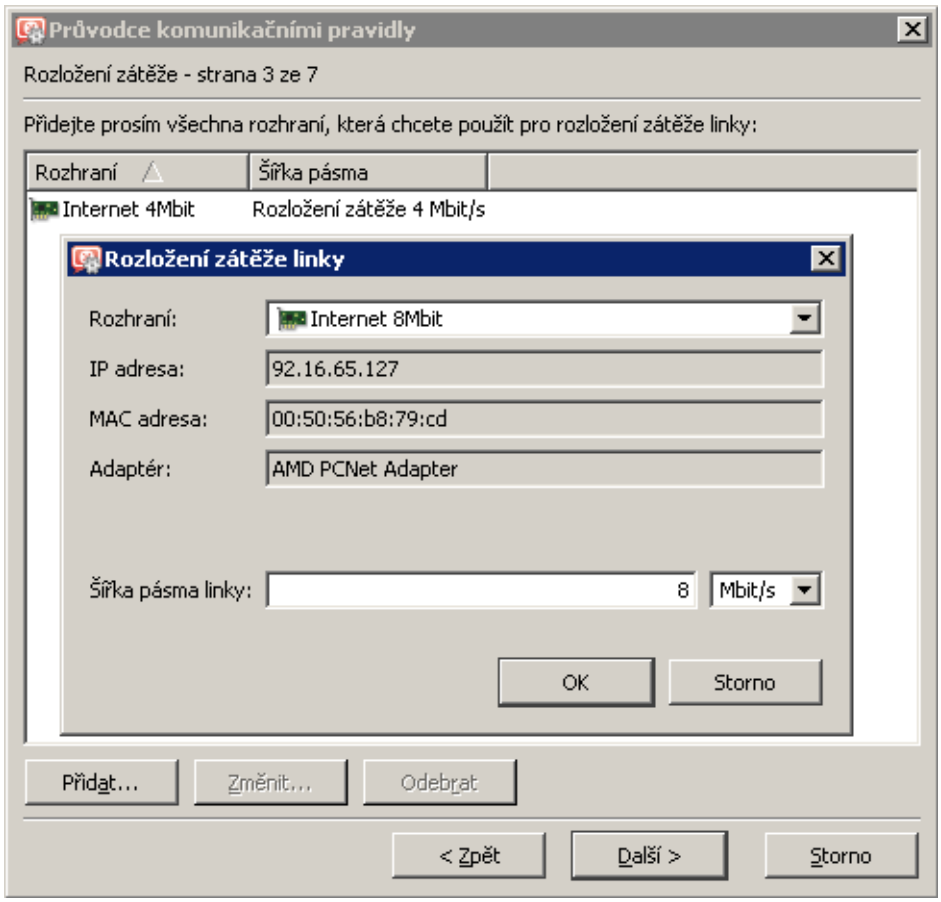
Obrázek 6.13 Průvodce komunikačními pravidly — rozložení zátěže internetového připojení

Ve třetím kroku průvodce pak postupně přidáme všechny linky, které chceme použít pro rozložení zátěže internetového připojení.

V edici *Software Appliance / VMware Virtual Appliance* je přímo v průvodci možné:

- Konfigurovat parametry vybraného rozhraní,
- Vytvořit nové rozhraní (*PPPoE*, *PPTP* nebo vytáčené připojení).

Podrobné informace o síťových rozhraních naleznete v kapitole 5.



Obrázek 6.14 Průvodce komunikačními pravidly — zálohování pevné linky vytáčeným připojením

Pro každou linku je třeba specifikovat šířku pásma, tj. rychlost linky. Na absolutní hodnotě rychlosti linky nezáleží (z důvodu přehlednosti by však měla pokud možno korespondovat s rychlostí linky udávanou poskytovatelem připojení). Důležitý je poměr mezi rychlostmi jednotlivých linek — ten udává, jakým způsobem bude internetová komunikace mezi tyto linky rozdělována.

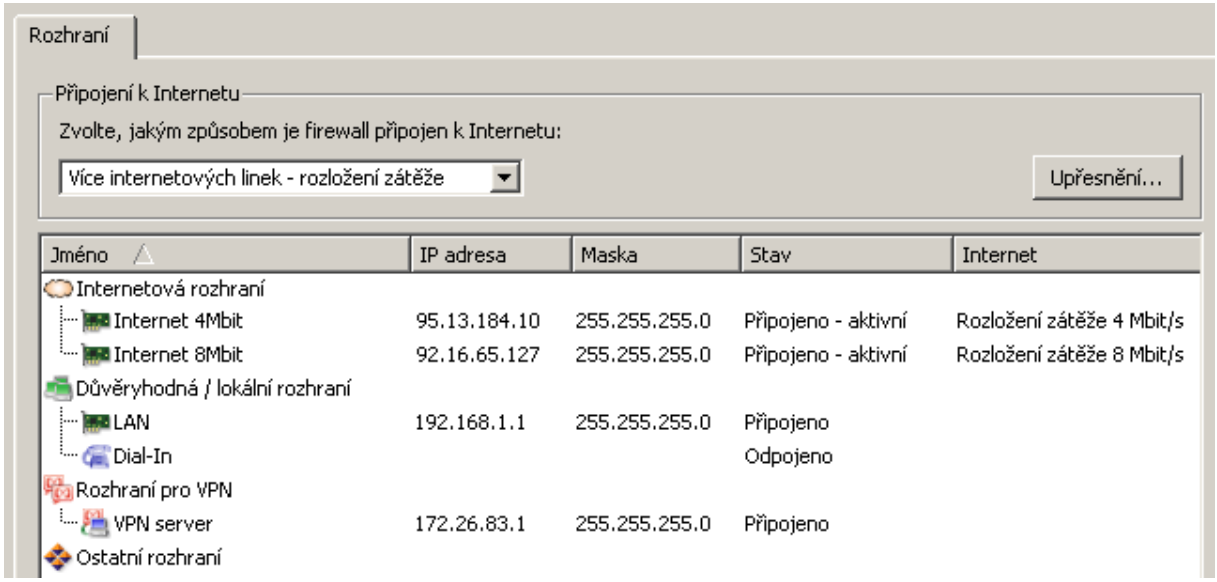
Pokud u vybraných telefonických připojení nejsou v operačním systému uloženy přihlašovací údaje, je třeba zadat příslušné jméno a heslo.

Příklad

Máme k dispozici dvě internetové linky. Jedné z nich nastavíme šířku pásma *4 Mbit/s* a druhé *8 Mbit/s*. Celková (deklarovaná) rychlost internetového připojení je tedy *12 Mbit/s*, přičemž třetinu této kapacity tvoří první linka a dvě třetiny druhá linka. Velmi zjednodušeně řečeno, třetina internetové komunikace bude směrována přes první linku a zbývající dvě třetiny přes druhou linku.

Výsledná konfigurace rozhraní

Po dokončení *Průvodce komunikačními pravidly* si můžeme v sekci *Konfigurace* → *Rozhraní* prohlédnout výslednou konfiguraci rozhraní a v případě potřeby ji dále upravit.



Obrázek 6.15 Konfigurace rozhraní — rozložení zátěže internetového připojení

Do skupiny *Internetová rozhraní* jsou zařazeny linky *Internet 4Mbit* a *Internet 8Mbit* vybrané ve třetím kroku průvodce jako rozhraní pro rozložení zátěže internetového připojení.

Ve sloupci *Internet* se zobrazují deklarované rychlosti jednotlivých linek (viz výše). Ve sloupci *Stav* je kromě stavu linky samotné (připojena/odpojena) zobrazována také informace, zda je linka aktivní — tzn. zda je internetové připojení touto linkou funkční a lze přes ni směrovat část internetové komunikace.

Ostatní rozhraní (včetně rozhraní *Dial-In*) jsou považována za segmenty lokální sítě a jsou zařazena do skupiny *Důvěryhodná / lokální rozhraní*.

Při přidání další linky do skupiny *Internetová rozhraní* bude nové lince nastavena výchozí rychlost (*1 Mbit/s*). Pak je vhodné upravit v dialogu pro změnu parametrů rozhraní (viz kapitola 5) deklarovanou rychlost linky s ohledem na její skutečnou rychlost, aby byla zátěž rozložena pokud možno rovnoměrně.

Tip

Rychlost linky (či několika linek) je možné nastavit i na *0 Mbit/s*. Takové linky pak nebudou použity pro rozložení zátěže internetového připojení, ale bude přes ně směrována pouze komunikace podle specifických komunikačních pravidel (viz kapitola 7.5). Zároveň však stále bude testována jejich dostupnost a tyto linky budou sloužit jako záložní pro případ výpadku všech ostatních linek.

Pokročilé nastavení (optimalizace, dedikované linky atd.)

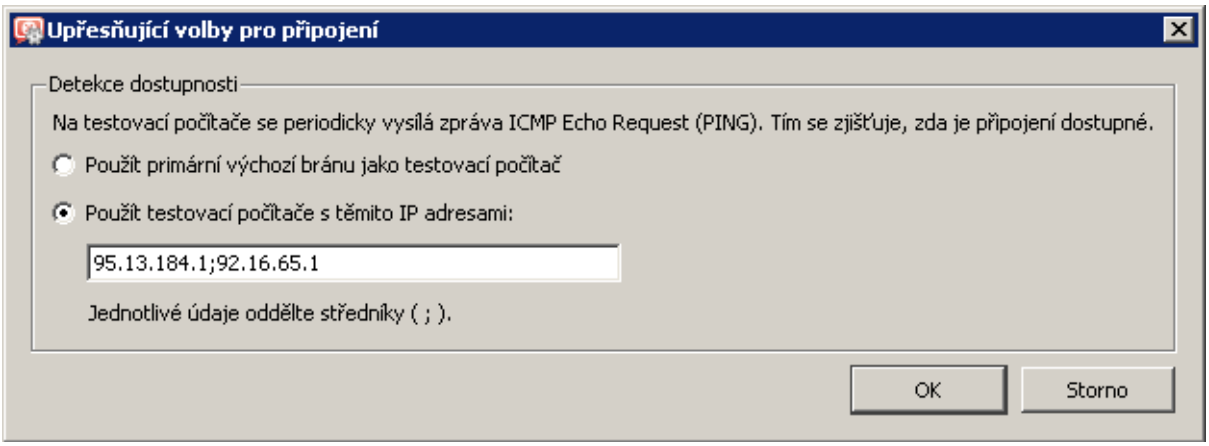
V základní konfiguraci probíhá rozložení zátěže sítě mezi jednotlivé linky automaticky podle jejich deklarovaných rychlostí (viz výše). Prostřednictvím komunikačních pravidel lze tento algoritmus upravit (např. vyhradit jednu linku pouze pro určitou komunikaci). Tato problematika je podrobně popsána v kapitole 7.5.

Testovací počítače

Funkčnost jednotlivých internetových linek se ověřuje periodickým vysíláním *ICMP* žádostí o odezvu (*PING*) na určité počítače nebo síťová zařízení. Standardně se jako testovací počítač používá výchozí brána příslušné linky. Je zřejmé, že pokud není výchozí brána dostupná, není příslušná linka (plně) funkční.

Pokud z nějakého důvodu nelze použít jako testovací počítač primární výchozí bránu (tzn. výchozí bránu nastavenou na testované lince), můžeme po stisknutí tlačítka *Upřesnění* specifikovat IP adresy jednoho nebo více testovacích počítačů. Je-li alespoň jeden z testovacích počítačů dostupný, považuje se internetové připojení za funkční.

Zadané testovací počítače budou použity při testování dostupnosti *všech* internetových linek. Proto by zde mělo být uvedeno několik počítačů z různých subsítí Internetu.



Obrázek 6.16 Rozložení zátěže internetového připojení — nastavení testovacích počítačů

Poznámka:

1. Testovací počítač nesmí blokovat zprávy *ICMP Echo Request* (*PING*), které *WinRoute* používá pro testování jeho dostupnosti — jinak by byl vždy vyhodnocen jako nedostupný. Toto je typický případ, kdy nelze použít výchozí bránu jako testovací počítač.

2. Jako testovací počítače je třeba použít počítače nebo síťová zařízení, která jsou trvale v provozu (např. servery, směrovače apod.). Použít jako testovací počítač pracovní stanici, která je v provozu několik hodin denně, nemá příliš velký smysl.

3. *ICMP* zprávy odesílané na testovací počítače nelze zablokovat komunikačními pravidly firewallu.

Kapitola 7

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 pro případy, kdy nejsou třeba žádná speciální nastavení).

Typický postup je vytvořit základní komunikační pravidla pomocí průvodce a tato pravidla pak „doladit“, případně doplnit další pravidla dle potřeby. Zkušení správci nemusejí průvodce použít vůbec — mohou vytvořit kompletní sadu pravidel přesně podle specifických požadavků.

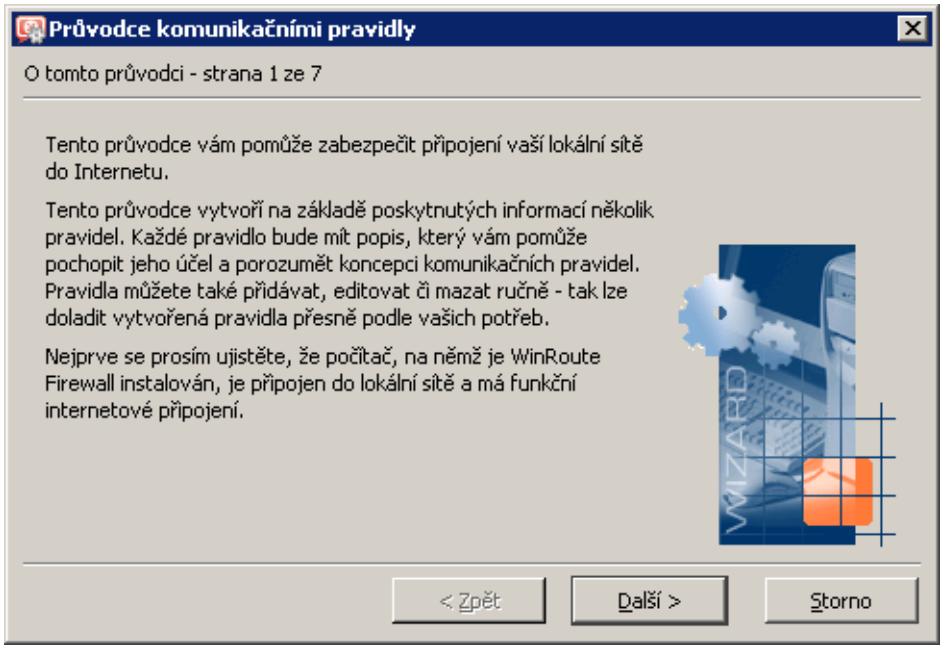
7.1 Průvodce komunikačními pravidly

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



Obrázek 7.1 Průvodce komunikačními pravidly — úvodní informace

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

- alespoň jedním aktivním adaptérem pro lokální síť
- alespoň jedním aktivním adaptérem připojeným k Internetu nebo je definováno alespoň jedno vytáčené připojení. Toto připojení nemusí být v okamžiku spuštění průvodce vytočeno.

Kroky 2 a 3 — nastavení internetového připojení

Ve druhém kroku průvodce zvolte požadovaný způsob připojení lokální sítě k Internetu pomocí *WinRoute* (pevná linka, vytáčené připojení, pevná linka se záložním připojením nebo více linek s rozložením zátěže).

Ve třetím kroku případně nastavte potřebné parametry pro zvolený typ internetového připojení.

Jednotlivé možnosti internetového připojení jsou podrobně popsány v kapitole 6.

Poznámka:

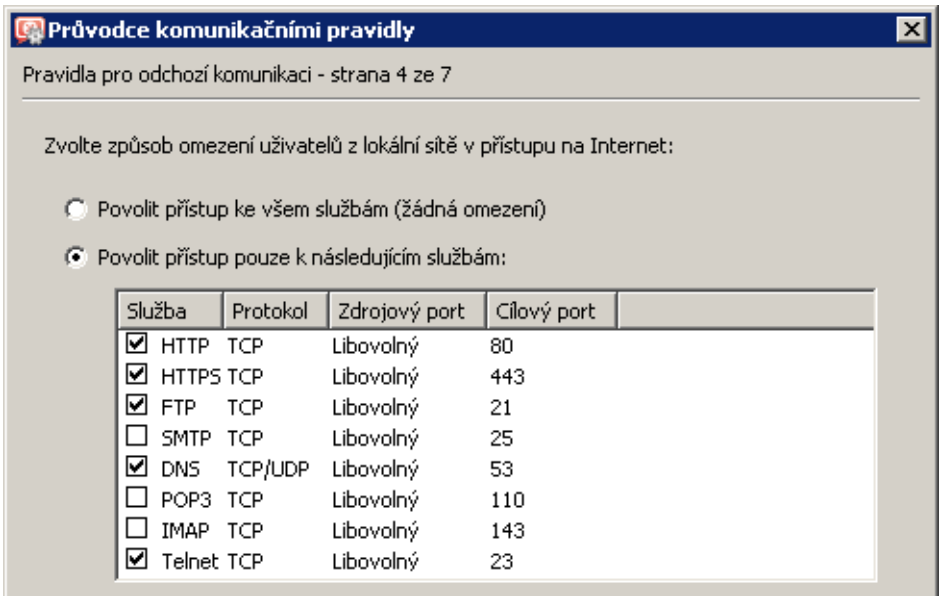
1. Výběr typu internetového připojení neovlivňuje výsledná komunikační pravidla, ale pouze konfiguraci rozhraní a jejich zařazení do skupin (viz kapitoly 5 a 6).

2. *Průvodce komunikačními pravidly* již neobsahuje volbu pro zapnutí / vypnutí překladu IP adres (NAT), která byla k dispozici ve starších verzích *WinRoute*. Ve vytvořených komunikačních pravidlech je nyní překlad adres automaticky vždy nastaven. Důvodem je

skutečnost, že režimy rozložení zátěže sítě, zálohování připojení a vytáčení na žádost prakticky nelze použít bez překladu adres.

Krok 4 — omezení přístupu na Internet

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



Obrázek 7.2 Průvodce komunikačními pravidly — povolení přístupu ke službám v Internetu

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:

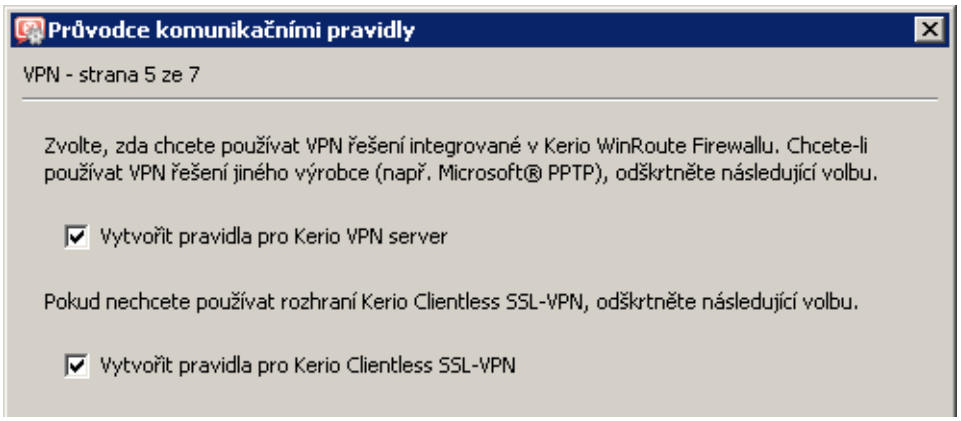
1. Nastavená omezení budou aplikována i na samotný firewall.
2. V tomto dialogu je uveden výčet pouze základních služeb (nezávisle na tom, jaké služby jsou ve *WinRoute* definovány — viz kapitola 14.3). Další služby lze povolit úpravou komunikačních pravidel *NAT* (pro počítače v lokální síti) nebo *Komunikace firewallu* (pro samotný firewall), případně přidáním vlastních pravidel. Podrobnosti viz kapitola 7.3.

Krok 5 — povolení komunikace Kerio VPN

Chcete-li použít proprietární VPN řešení ve *WinRoute* pro připojování vzdálených klientů nebo vytváření tunelů mezi vzdálenými sítěmi, ponechte zapnutou volbu *Vytvořit pravidla pro Kerio VPN server*. Průvodce přidá do komunikačních pravidel specifické služby a skupiny adres pro *Kerio VPN*. Podrobné informace o proprietárním VPN řešení naleznete v kapitole 23.

Používáte-li (nebo plánujete-li použít) VPN řešení jiného výrobce (např. *Microsoft PPTP*, *Nortel IPSec* apod.), vypněte volbu *Vytvořit pravidla pro Kerio VPN server*.

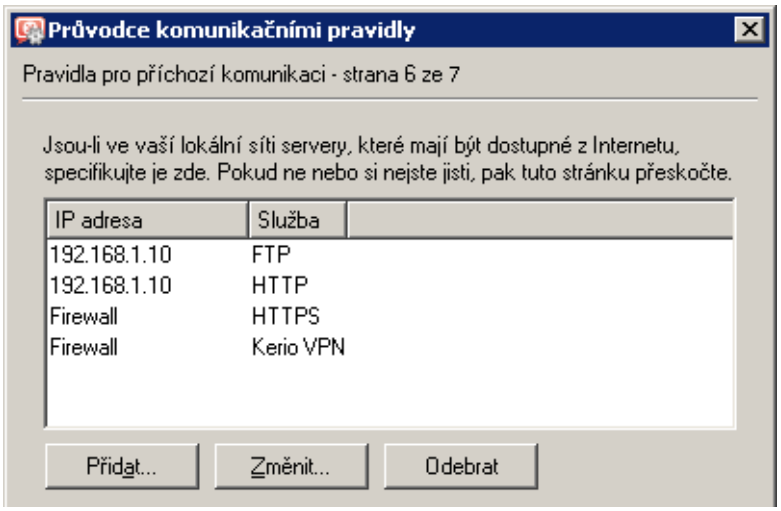
Chcete-li vzdáleně přistupovat ke sdíleným prostředkům v lokální síti pomocí WWW prohlížeče, ponechte zapnutou volbu *Vytvořit pravidla pro Kerio Clientless SSL-VPN*. Toto rozhraní je nezávislé na *Kerio VPN* a může být použito i společně s VPN řešením jiného výrobce. Podrobné informace naleznete v kapitole 24.



Obrázek 7.3 Průvodce komunikačními pravidly — Kerio VPN

Krok 6 — zpřístupnění služeb v lokální síti

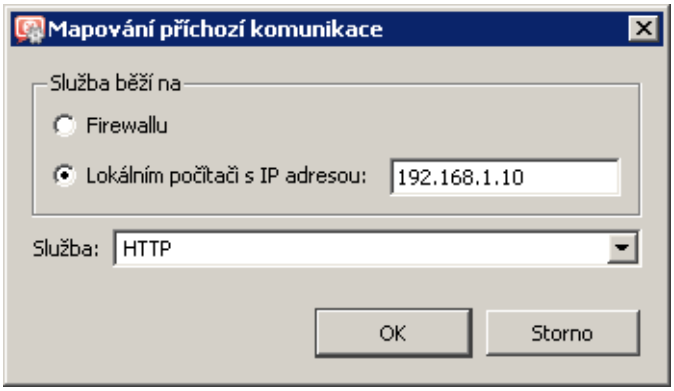
Je-li na počítači s *WinRoute* či na některém počítači v lokální síti provozována služba (např. WWW server, FTP server apod.), kterou chcete zpřístupnit z Internetu, definujte ji v tomto dialogu.



Obrázek 7.4 Průvodce komunikačními pravidly — zpřístupnění lokálních služeb

Poznámka: Pokud bylo v předchozím kroku požadováno vytvoření pravidel pro VPN, budou do seznamu lokálních serverů automaticky přidány služby *Kerio VPN* a *HTTPS* na firewallu. Odstranění nebo změna nastavení těchto služeb způsobí nedostupnost VPN služeb z Internetu!

Tlačítko *Přidat* otevírá dialog pro zpřístupnění nové služby.



Obrázek 7.5 Průvodce komunikačními pravidly — mapování lokální služby

Služba běží na

Volba počítače, na kterém běží příslušná služba (tzn. na který bude přesměrována příchozí komunikace z Internetu):

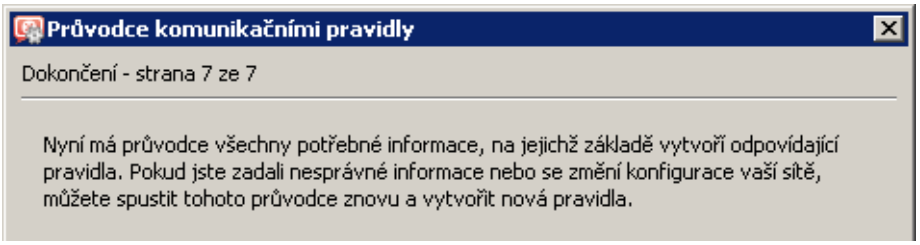
- *Firewall* — počítač, na němž je *WinRoute* nainstalován
- *Lokální počítač s IP adresou* — jiný počítač v lokální síti (lokální server)
  Poznámka: Výchozí brána na lokálním serveru musí být nastavena tak, aby přistupoval do Internetu přes *WinRoute* — jinak nebude zpřístupnění služby fungovat!

Služba

Výběr služby, která má být zpřístupněna. Tato služba musí být nejprve definována v sekci *Konfigurace* → *Definice* → *Služby* (viz kapitola 14.3). Většina běžných služeb je ve *WinRoute* již předdefinována.

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.



Obrázek 7.6 Průvodce komunikačními pravidly — dokončení

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.

Tato pravidla jsou nezávislá na zvoleném způsobu internetového připojení (2. a 3. krok průvodce).

Jméno	Zdroj	Cíl	Služba	Akce	Překlad
Služba FTP	Libovolný	Firewall	FTP	✓	Mapování 192.168.1.10
Služba HTTP	Libovolný	Firewall	HTTP	✓	Mapování 192.168.1.10
Služba HTTPS	Libovolný	Firewall	HTTPS	✓	
Služba Kerio VPN	Libovolný	Firewall	Kerio VPN	✓	
NAT	Důvěryhodné / lokální	Internet	DNS FTP HTTP HTTPS Telnet	✓	NAT
Lokální komunikace	Firewall Všichni VPN klienti Všechny VPN tunely Důvěryhodné / lokální	Firewall Všichni VPN klienti Všechny VPN tunely Důvěryhodné / lokální	Libovolný	✓	
Komunikace firewallu	Firewall	Libovolný	DNS FTP HTTP HTTPS Telnet	✓	
Výchozí pravidlo	Libovolný	Libovolný	Libovolný	✗	

Obrázek 7.7 Komunikační pravidla vytvořená průvodcem

Služba FTP a Služba HTTP

Tato dvě pravidla zpřístupňují (mapují) služby *HTTP* a *HTTPS* běžící na počítači s IP adresou `192.168.1.10` (krok 6). Tyto služby budou přístupné na IP adresách „vnějšího“ rozhraní firewallu (tj. rozhraní připojeného k Internetu — krok 3).

Poznámka: Od verze *WinRoute 6.4.0* lze na mapované služby přistupovat také z lokální sítě — není již tedy nutné při přístupu z lokálních klientů používat jinou (privátní) IP adresu. Z tohoto důvodu je v položce *Zdroj* nastavena hodnota *Libovolný*. Podrobnosti viz kapitola 7.3.

Služba Kerio VPN a Služba HTTPS

Pravidlo *Služba Kerio VPN* povoluje připojení k VPN serveru ve *WinRoute* (navázání řídicího spojení mezi VPN klientem a serverem, resp. vytvoření VPN tunelu — podrobnosti viz kapitola 23).

Pravidlo *Služba HTTPS* povoluje připojení k rozhraní *Clientless SSL-VPN* (přístup ke sdíleným prostředkům v síti pomocí WWW prohlížeče — podrobnosti viz kapitola 24).

Každé z těchto pravidel je vytvořeno pouze v případě, pokud bylo v kroku 5 průvodce komunikačními pravidly požadováno povolení přístupu k příslušné službě.

Poznámka: V těchto pravidlech je rovněž v položce *Zdroj* nastavena hodnota *Libovolný*. Hlavním důvodem je udržení konzistence s pravidly pro mapované služby (všechna tato pravidla se vytvářejí v 6. kroku průvodce). Přístup z lokální sítě ke službám na firewallu je za normálních okolností povolen pravidlem *Komunikace firewallu*, ale nemusí tomu tak být vždy.

NAT

Toto pravidlo určuje, že ve všech paketech směrovaných z lokální sítě do Internetu bude zdrojová (privátní) IP adresa nahrazována adresou internetového rozhraní, přes které je paket z firewallu odesílán. Přístup do Internetu bude povolen pouze k vybraným službám (4. krok průvodce).

Položka *Zdroj* tohoto pravidla obsahuje skupinu *Důvěryhodná / lokální rozhraní* a položka *Cíl* obsahuje skupinu *Internetová rozhraní*. Díky tomu je pravidlo zcela univerzální pro libovolnou konfiguraci sítě. Při připojení nového segmentu lokální sítě či změně internetového připojení není nutné toto pravidlo měnit.

Skupina *Důvěryhodná / lokální rozhraní* standardně obsahuje také adaptér *Dial-In*, tzn. všichni klienti služby *RAS* připojující se na tento server budou mít povolen přístup do Internetu pomocí technologie *NAT*.

Lokální komunikace

Toto pravidlo povoluje veškerou komunikaci počítačů v lokální síti firewallem (tj. s počítačem, na němž je *WinRoute* nainstalován). Položky *Zdroj* a *Cíl* v tomto pravidle zahrnují skupinu *Důvěryhodná / lokální rozhraní* (viz kapitola 5) a speciální skupinu *Firewall*.

Skupina *Důvěryhodná / lokální rozhraní* standardně obsahuje také adaptér *Dial-In*. Pravidlo *Lokální komunikace* tedy povoluje také komunikaci mezi počítači v lokální síti (resp. firewallem) a klienty služby *RAS* připojujícími se na tento server.

Pokud bylo v průvodci požadováno vytvoření pravidel pro *Kerio VPN* (5. krok průvodce), pak pravidlo *Lokální komunikace* obsahuje také speciální skupiny adres *Všechny VPN tunely* a *Všichni VPN klienti*. Pravidlo tedy implicitně povoluje komunikaci mezi lokální sítí (firewallem), vzdálenými sítěmi připojenými přes VPN tunely a VPN klienty připojujícími se k VPN serveru ve *WinRoute*.

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 mezi lokální sítí a Internetem 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).

Výchozí pravidlo
: Toto pravidlo zahazuje 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: Podrobný popis jednotlivých částí komunikačního pravidla najdete v kapitole 7.3.

7.2 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:

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

2. Pro řízení přístupu uživatelů k WWW a FTP serverům a filtrování obsahu doporučujeme namísto komunikačních pravidel použít speciální nástroje, které *WinRoute* k tomuto účelu nabízí — viz kapitola 12.

7.3 Definice vlastních komunikačních pravidel

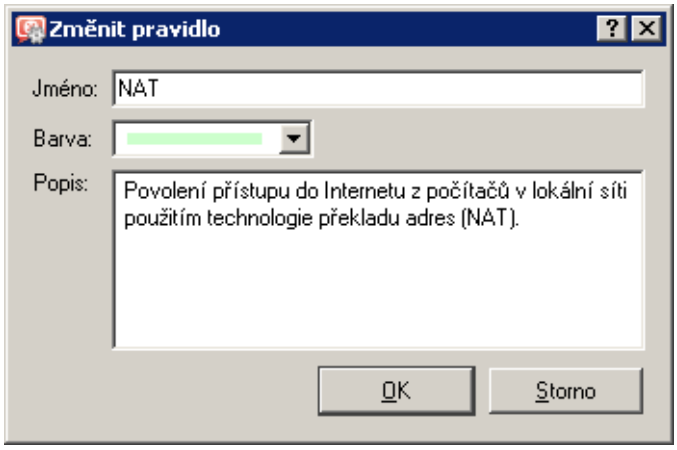
Komunikační pravidla jsou zobrazována ve formě tabulky, kde každý řádek obsahuje jedno pravidlo a ve sloupcích jsou jeho jednotlivé části (jméno, podmínky, akce — podrobnosti viz dále). Dvojitým kliknutím levým tlačítkem myši na vybrané pole tabulky (případně kliknutím pravým tlačítkem a volbou *Změnit...* 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.



Obrázek 7.8 Komunikační pravidlo — jméno, barva a popis pravidla

Kromě jména lze 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). Barevné označení umožňuje zvýraznit některá pravidla nebo odlišit určité skupiny pravidel (např. pravidla pro odchozí a pro příchozí komunikaci).

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

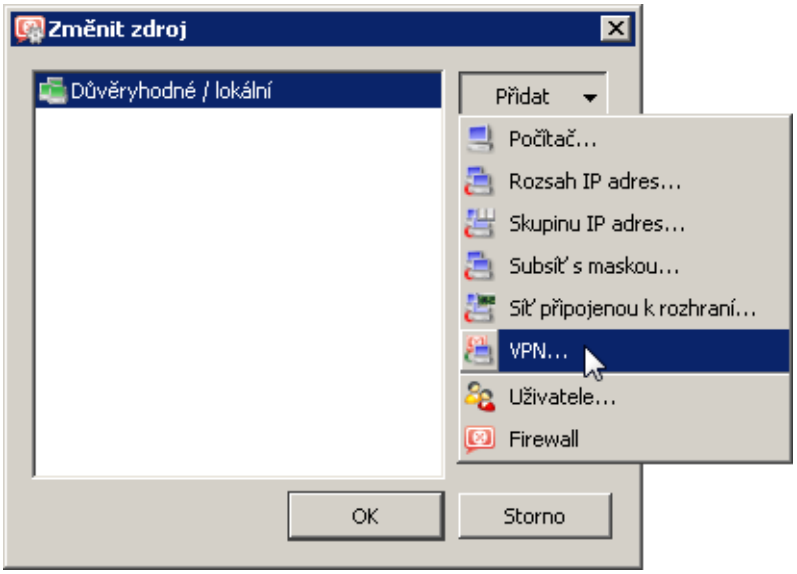
Je-li popis uveden, pak se v seznamu pravidel ve sloupci *Jméno* vedle názvu pravidla zobrazí symbol „bubliny“. Umístěním kurzoru myši na tento symbol bude zobrazen text popisu pravidla.

Doporučujeme důsledně popisovat všechna vytvořená pravidla (v pravidlech vytvořených průvodcem je popis již vyplněn). 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.

Poznámka: Popis a barevné označení pravidla slouží pouze pro zlepšení přehlednosti — nemají vliv na činnost firewallu.

Zdroj, Cíl

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



Obrázek 7.9 Komunikační pravidlo — definice zdrojových adres

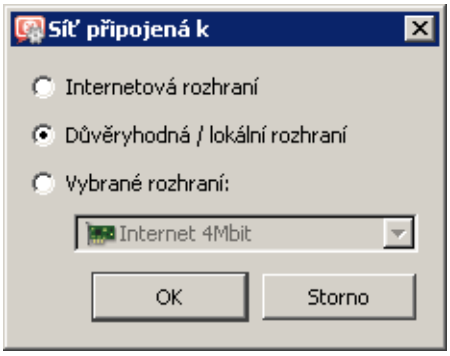
Tlačítkem *Přidat* lze definovat novou položku zdroje, resp. cíle komunikace:

- *Počítač* — jméno nebo IP adresa konkrétního počítače (např. `www.firma.cz` nebo `192.168.1.1`)

  Upozornění

  Je-li zdrojový nebo cílový počítač zadán DNS jménem, pak *WinRoute* zjišťuje odpovídající IP adresu v okamžiku stisknutí tlačítka *Použít*.
  Pokud není nalezen odpovídající záznam v DNS cache, vysílá se DNS dotaz do Internetu. Je-li internetové připojení realizováno vytáčenou linkou, která je momentálně zavěšena, vyšle se tento dotaz až po vytočení linky. Do zjištění IP adresy z DNS jména je však příslušné pravidlo neaktivní. V krajním případě může dojít i k tomu, že po definici pravidla bude linka vytočena na základě komunikace, která má být pravidlem zakázána.
  Z výše uvedených důvodů doporučujeme v případě vytáčené internetové linky zadávat zdrojové a cílové počítače výhradně IP adresami!

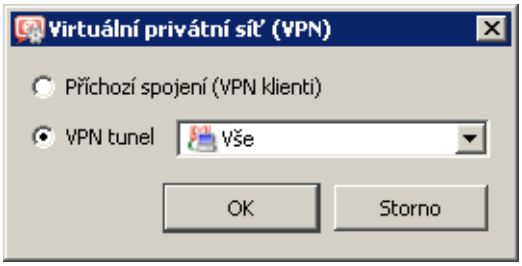
- *Rozsah IP adres* — např. `192.168.1.10—192.168.1.20`
- *Skupinu IP adres* — skupina adres definovaná ve *WinRoute* (viz kapitola 14.1)
- *Subsíť s maskou* — subsíť zadaná adresou sítě a maskou
  (např. `192.168.1.0/255.255.255.0`)
- *Síť připojenou k rozhraní* — výběr rozhraní nebo skupiny rozhraní, odkud paket přichází (v položce *Zdroj*) nebo kudy má být odeslán (v položce *Cíl*).
  Skupiny rozhraní umožňují vytvářet obecnější pravidla, která jsou nezávislá na konkrétní konfiguraci sítě (např. při změně internetového připojení nebo přidání segmentu lokální sítě není nutné taková pravidla měnit). Je-li to možné, doporučujeme definovat komunikační pravidla s použitím skupin rozhraní. Podrobnosti o síťových rozhraních a skupinách rozhraní viz kapitola 5.
  Poznámka: V komunikačních pravidlech lze použít pouze skupiny *Internetová roz-*



Obrázek 7.10 Komunikační pravidlo — výběr rozhraní nebo skupiny rozhraní

hraní a *Důvěryhodná / lokální rozhraní*. Rozhraní pro *Kerio VPN* se přidávají jiným způsobem (viz níže). Skupina *Ostatní rozhraní* obsahuje rozhraní různých typů, která nebyla zařazena do jiné skupiny. Komunikační pravidlo pro tuto skupinu jako celek by ve většině případů nemělo žádný smysl.

- *VPN* — virtuální privátní síť (vytvořená pomocí *Kerio VPN*). Volbou *VPN* můžeme přidat položky následujících typů:

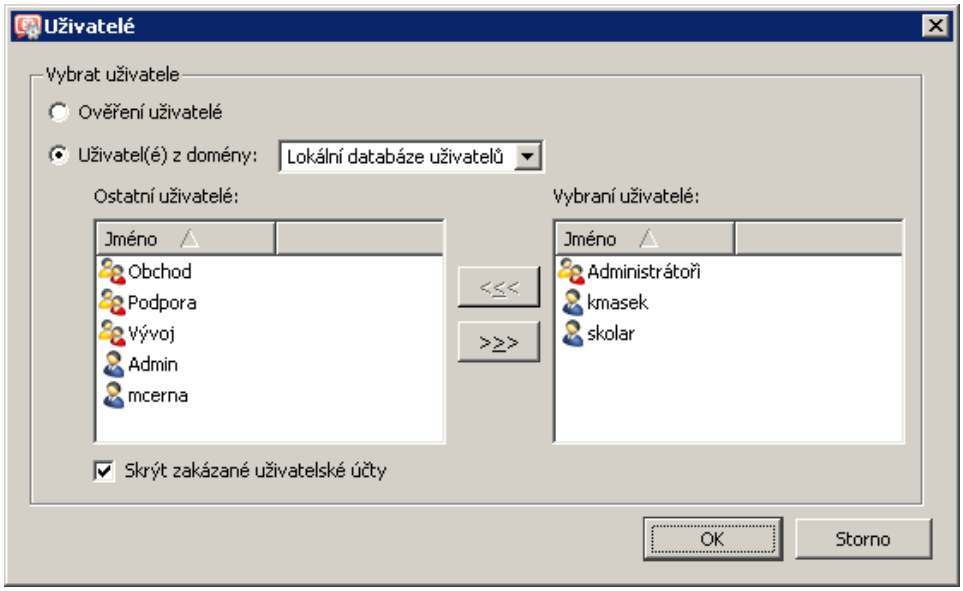


Obrázek 7.11 Komunikační pravidlo — VPN klienti / VPN tunel v definici zdrojových nebo cílových adres

1. *Příchozí spojení (VPN klienti)* — všichni VPN klienti připojující se k VPN serveru ve *WinRoute* pomocí aplikace *Kerio VPN Client*,
2. *VPN tunel* — síť připojená vybraným VPN tunelem. Speciální volba *Vše* znamená všechny sítě připojené všemi definovanými VPN tunely (které jsou v daném okamžiku aktivní).

Podrobné informace o VPN řešení ve *WinRoute* naleznete v kapitole 23.

- *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 10.1). Volbou *Uživatelé z domény* můžeme přidat požadované uživatele a/nebo skupiny z mapovaných *Active Directory* domén nebo z lokální databáze uživatelů (podrobnosti viz kapitola 15).



Obrázek 7.12 Komunikační pravidlo — uživatelé a skupiny v definici zdrojových nebo cílových adres

Tip

Do pravidla můžeme přidat uživatele/skupiny z několika různých domén zároveň. Vybereme doménu, přidáme uživatele a/nebo skupiny, pak zvolíme jinou doménu a postup opakujeme.

V komunikačních pravidlech má uživatel význam IP adresy počítače, z něhož je přihlášen. Podrobnosti o přihlašování uživatelů k firewallu naleznete v kapitole 10.1.
Poznámka:

1. Povolení / zákaz přístupu určitým uživatelům má smysl jen tehdy, pokud není z příslušných IP adres povolen přístup nepřihlášeným uživatelům (jinak totiž nejsou uživatelé donuceni se přihlásit). Pokud uživatelé pracují střídavě na různých počítačích, je třeba vzít v úvahu IP adresy všech těchto počítačů.
2. Jsou-li uživatelské účty nebo skupiny použity jako zdroj v pravidle pro přístup do Internetu, pak v případě služby HTTP nebude funkční automatické přesměrování uživatelů na přihlašovací stránku ani NTLM ověřování. K přesměrování totiž dojde až po úspěšném navázání spojení na cílový server.
   Jsou-li komunikační pravidla nastavena tímto způsobem, pak je třeba uživatelům sdělit, že před přístupem do Internetu musejí otevřít přihlašovací stránku (viz kapitoly 11 a 10.1) ve svém WWW prohlížeči a přihlásit se.
   Tato problematika je podrobně diskutována v kapitole 7.6.

- *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*.

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.

Tlačítko *Smazat* odstraní všechny definované položky (v seznamu položek bude zobrazeno *Nic*). Toto je užitečné při změně pravidel — není nutné odstraňovat postupně jednotlivé položky. Bude-li pak přidána alespoň jedna nová položka, bude hodnota *Nic* automaticky odstraněna. Ponecháme-li ve sloupci *Zdroj* a/nebo *Cíl* hodnotu *Nic*, pak bude pravidlo neaktivní.

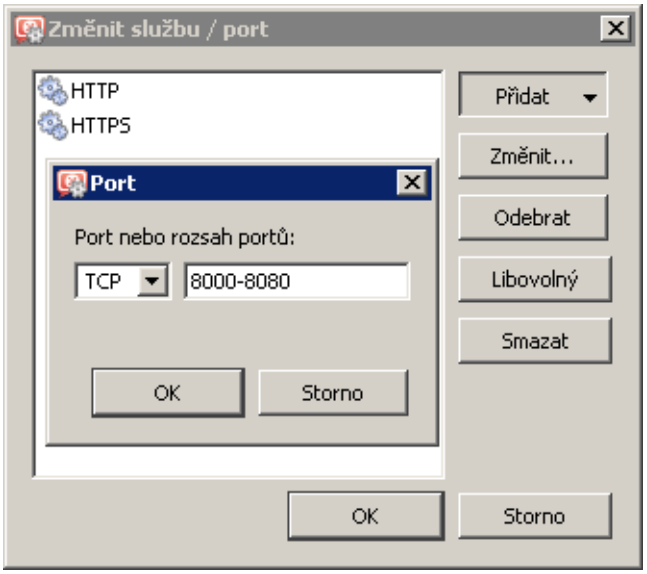
Hodnota *Nic* má své opodstatnění při odstranění síťových rozhraní (viz kapitola 5) a uživatelských účtů nebo skupin (viz kapitola 15). Do položek *Zdroj*, *Cíl* nebo *Služba* všech pravidel, ve kterých bylo použito odstraněné rozhraní, (resp. uživatelský účet, skupina nebo služba) bude automaticky dosazena hodnota *Nic*, čímž budou příslušná pravidla deaktivována.

Definice pravidla s hodnotou *Nic* v některém sloupci nemá praktický význam — pro deaktivaci pravidla je vhodnější použít zaškrtávací pole ve sloupci *Jméno*.

Poznámka: Odstraněné rozhraní nelze nahradit položkou *Libovolný* — mohlo by dojít k zásadní změně smyslu komunikačních pravidel (např. povolení nežádoucí komunikace).

Služba

Definice služby (resp. služeb), pro kterou má toto komunikační pravidlo platit. Seznam může obsahovat více služeb definovaných v sekci *Konfigurace* → *Definice* → *Služby* (viz kapitola 14.3) a/nebo služeb zadaných protokolem a číslem portu (případně rozsahem portů — pro jeho specifikaci se zde používá pomlčka).



Obrázek 7.13 Komunikační pravidlo — nastavení služby

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.

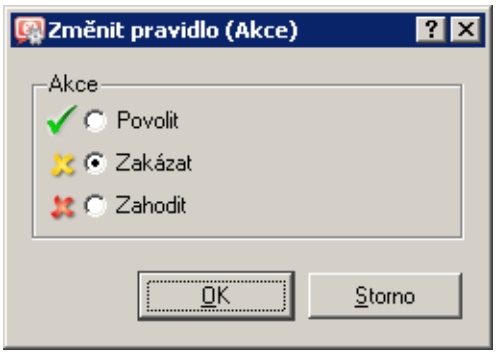
Tlačítko *Smazat* odstraní všechny definované položky (v seznamu položek bude zobrazeno *Nic*). Bude-li pak přidána alespoň jedna nová služba, bude hodnota *Nic* automaticky odstraněna. Ponecháme-li ve sloupci *Služba* hodnotu *Nic*, pak bude pravidlo neaktivní.

Hodnota *Nic* má své opodstatnění při odstraňování definovaných služeb (viz kapitola 14.3). Do položky *Služba* všech pravidel, ve kterých byla použita odstraněná služba, bude automaticky dosazena hodnota *Nic*, čímž budou příslušná pravidla deaktivována. Ruční dosazení hodnoty *Nic* nemá praktický význam — pro deaktivaci pravidla je vhodnější použít zaškrtávací pole ve sloupci *Jméno*.

Poznámka: Existuje-li ve *WinRoute* pro určitou službu inspekční modul, pak se tento modul automaticky aplikuje na veškerou odpovídající komunikaci. Chceme-li docílit toho, aby na určitou komunikaci nebyl aplikován příslušný inspekční modul, je třeba to v komunikačním pravidle explicitně uvést. Podrobné informace viz kapitola 7.7.

Akce

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



Obrázek 7.14 Komunikační pravidlo — volba akce

- *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 ten tuto situaci vyhodnotí jako síťovou chybu. Odezva klienta není v tomto případě okamžitá (klient 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*.

Překlad

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

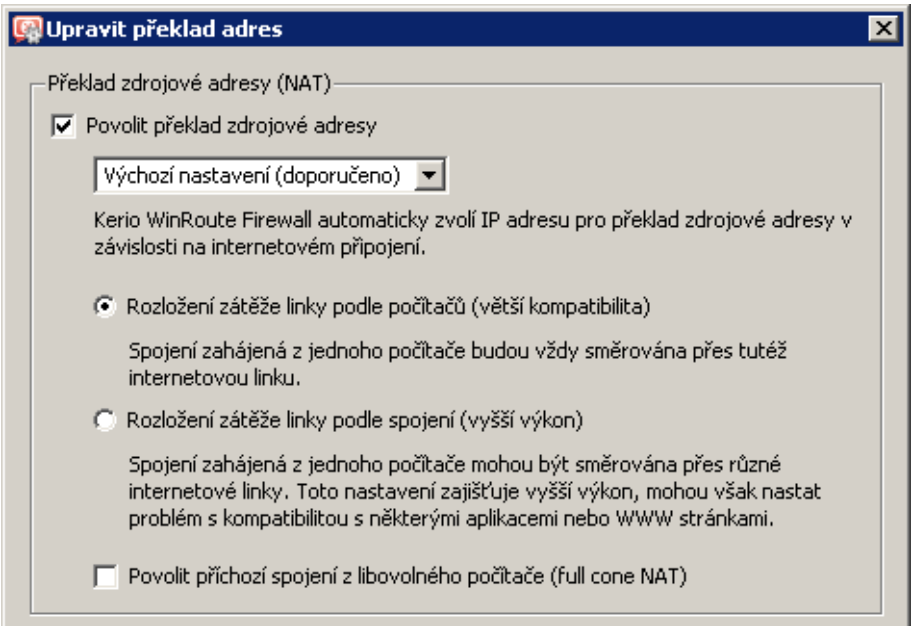
Překlad zdrojové IP adresy (NAT — sdílení internetového připojení)

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

Překlad zdrojové adresy se používá v komunikačních pravidlech, která se aplikují na komunikaci z lokální privátní sítě do Internetu. V ostatních pravidlech (komunikace mezi lokální sítí a firewallem, mezi firewallem a Internetem apod.) nemá překlad zdrojové adresy smysl. Podrobnější informace včetně příkladů pravidel naleznete v kapitole 7.4.

Pro překlad zdrojové adresy nabízí *WinRoute* tyto možnosti:

Automatický výběr IP adresy



Obrázek 7.15 Komunikační pravidlo — NAT — automatický výběr adresy

Ve výchozím nastavení bude v paketech odesílaných z lokální sítě do Internetu nahrazena zdrojová IP adresa IP adresou internetového rozhraní firewallu, přes které je paket odesílán. Tento způsob překladu IP adres je optimální pro použití v obecném pravidle pro přístup z lokální sítě do Internetu (viz kapitola 7.4), protože funguje správně při libovolné konfiguraci internetového připojení a stavu jednotlivých linek (podrobnosti viz kapitola 6).

Pokud *WinRoute* pracuje v režimu rozložení zátěže internetového připojení (viz kapitola 6.4), můžeme zvolit způsob, jakým bude komunikace mezi lokální sítí a Internetem „rozdělována“ mezi jednotlivé internetové linky:

- *Rozložení podle zdrojových počítačů* — veškerá komunikace z konkrétního počítače (klienta) v lokální síti bude směrována vždy toutéž internetovou linkou.

Všechna spojení z daného klienta budou navázána ze stejné zdrojové IP adresy (veřejné adresy příslušného rozhraní firewallu). Tento způsob je nastaven jako výchozí, protože zaručuje stejné chování jako v případě klienta připojeného přímo k Internetu. Rozložení zátěže mezi jednotlivé linky však nemusí být optimální.

- *Rozložení podle spojení* — pro každé spojení navazované z lokální sítě do Internetu bude vybrána internetová linka tak, aby zátěž byla rozložená optimálně. Tento způsob zajišťuje maximální využití kapacity internetového připojení, může však docházet k problémům s některými službami. Jednotlivá spojení jsou totiž navazována z různých zdrojových IP adres (podle rozhraní, ze kterého byl paket z firewallu odeslán), což může server vyhodnotit jako útok a v důsledku toho ukončit relaci, blokovat komunikaci apod.

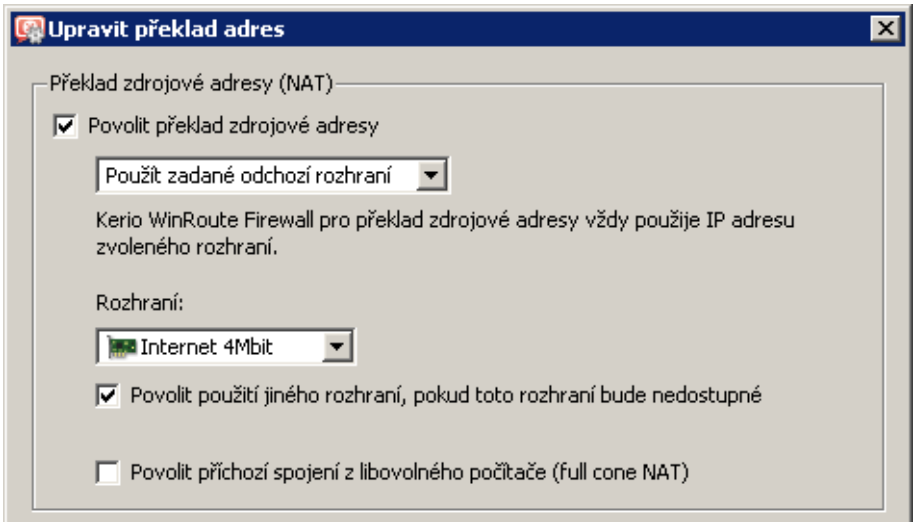
Je-li použit jiný typ internetového připojení (jedna pevná linka, vytáčení na žádost nebo zálohované připojení), nemají tyto volby na činnost *WinRoute* žádný vliv.

Tip

Pro maximální využití kapacity připojení můžeme použít kombinaci obou způsobů rozložení zátěže. V obecném pravidle pro přístup z lokání sítě do Internetu použijeme rozložení podle spojení a přidáme pravidlo pro specifické služby (servery, klienty apod.), ve kterém bude použito rozložení zátěže podle počítačů. Viz též kapitola 7.4.

Překlad na adresu vybraného rozhraní

Pro NAT můžeme vybrat konkrétní rozhraní, na jehož IP adresu bude zdrojová adresa v odchozích paketech překládána. Tím je zároveň dáno, že pakety budou do Internetu odesílány právě přes tuto linku. Takto lze definovat pravidla pro odesílání určité komunikace přes vybrané rozhraní — tzv. *policy routing* — viz kapitola 7.5.



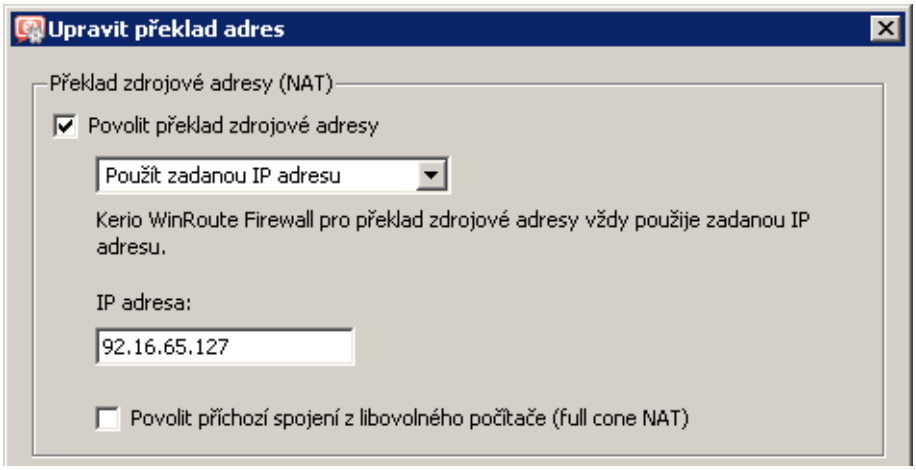
Obrázek 7.16 Komunikační pravidlo — NAT — překlad na adresu vybraného rozhraní

Pokud by došlo k výpadku vybrané internetové linky, pak by pro komunikaci vyhovující tomuto pravidlu (specifické služby, klienti apod.) byl Internet nedostupný. Pro ošetření této situace je možné povolit použití jiného rozhraní (linky) při výpadku vybrané linky. *WinRoute* se pak bude po dobu trvání výpadku chovat stejně jako v případě automatického výběru rozhraní (viz výše).

Překlad na zadanou IP adresu

Pro NAT může být zadána IP adresa, která bude použita jako zdrojová adresa ve všech paketech odesílaných z lokální sítě do Internetu. Tato možnost slouží především pro zachování kompatibility se staršími verzemi *WinRoute*. Použití pevné IP adresy má však značná omezení:

- Je nutné použít IP adresu některého z internetových rozhraní firewallu. Při použití jiné adresy (či dokonce lokální privátní adresy) nebude překlad IP adres fungovat správně a pakety odeslané do Internetu budou zahazovány.
- Ze zřejmých důvodů nelze specifickou IP adresu použít v režimech zálohování internetového připojení a rozložení zátěže.



Obrázek 7.17 Komunikační pravidlo — NAT — překlad na zadanou IP adresu

Full cone NAT

Při všech způsobech překladu IP adres je možné nastavit režim povolení příchozích paketů z libovolné adresy — tzv. *Full cone NAT*.

Je-li tato volba vypnuta, pak *WinRoute* provádí tzv. *Port restricted cone NAT*. V odchozích paketech z lokální sítě do Internetu zamění zdrojovou IP adresu za veřejnou IP adresu příslušného rozhraní firewallu (viz výše). Pokud je to možné, zachová původní zdrojový port, v opačném případě přidělí jiný volný zdrojový port. V příchozím směru pak propustí pouze pakety vyslané ze stejné IP adresy a portu, na který byl odeslán odchozí paket. Tento způsob překladu zaručuje vysokou bezpečnost — firewall nepropustí do lokální sítě žádný paket, který není odpovědí na vyslaný požadavek.

Řada aplikací (zejména programy pro multimédia, internetovou telefonii — VoIP apod.) však často používá model komunikace, kdy se k portu „otevřenému“ odchozím paketem mohou

připojit další klienti pro navázání přímého spojení. Proto *WinRoute* podporuje také režim *Full cone NAT*, kde neplatí uvedené omezení pro příchozí pakety. Na daném portu jsou pak propouštěny příchozí pakety s libovolnou zdrojovou IP adresou a portem. Tento způsob překladu umožňuje provozovat v privátní síti aplikace, které by za normálních okolností fungovaly omezeně nebo nefungovaly vůbec.

Příklad použití *Full cone NAT* pro VoIP aplikace naleznete v kapitole 7.8.

Upozornění

Použití *Full cone NAT* představuje značné bezpečnostní riziko — k portu otevřenému odchozím spojením je povolen přístup bez omezení. Z tohoto důvodu doporučujeme povolovat *Full cone NAT* pouze pro konkrétní službu (pro tento účel vytvoříme speciální komunikační pravidlo).

V žádném případě nepovolujte Full cone NAT v obecném pravidle pro komunikaci z lokální sítě do Internetu[4]*!* Takové pravidlo by znamenalo výraznou degradaci zabezpečení lokální sítě.

Poznámka:

1. Starší verze *WinRoute* (do verze *6.3.1* včetně) prováděly tzv. symetrický překlad (*Symmetric NAT*), kdy byl každému odchozímu spojení na firewallu přidělen nový zdrojový port z vyhrazeného rozsahu. Z tohoto důvodu poskytuje *WinRoute* od verze *6.4.0* výrazně lepší podporu VoIP a multimediálních aplikací než předchozí verze, i bez speciálních komunikačních pravidel. Oba způsoby překladu jsou stejně bezpečné — liší se pouze způsobem přiřazování zdrojových portů na firewallu.

2. Způsob překladu IP adres použitý od verze *6.4.0* (tj. *Port restricted cone NAT*) umožňuje také použití protokolu *IPSec*. Speciální podpora pro IPSec, obsažená ve starších verzích *WinRoute*, již není potřeba.

Překlad cílové adresy (mapování portů)

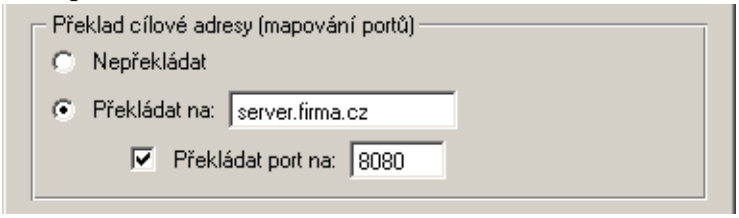
Překlad cílové adresy (též mapování portů) slouží ke zpřístupnění služby běžící na počítači v privátní lokální síti z Internetu. Pokud příchozí paket vyhovuje daným podmínkám, je cílová adresa zaměněna a paket směrován na příslušný počítač. Tímto způsobem bude služba „přenesena“ na internetové rozhraní 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 veřejné IP adrese firewallu).

Nastavení překladu cílové adresy (mapování portů):

- *Nepřekládat* — cílová adresa zůstane nezměněna.
- *Překládat na* — IP adresa, na níž má být cílová adresa paketu změněna. Tato adresa je zároveň adresou počítače, kde daná služba skutečně běží.

[4] Typicky pravidlo *NAT* vytvořené *Průvodcem komunikačními pravidly* — viz kapitola 7.1.

Do položky *Překládat na* lze rovněž uvést DNS jméno cílového počítače. V tom případě zjistí *WinRoute* příslušnou IP adresu DNS dotazem.



Obrázek 7.18 Komunikační pravidlo — překlad cílové adresy

Upozornění

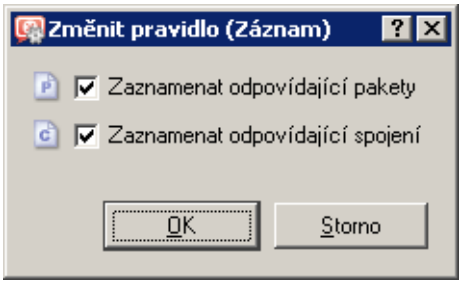
Nedoporučujeme zadávat jména počítačů, pro které neexistuje záznam v lokálním DNS. Do zjištění odpovídající IP adresy je totiž příslušné pravidlo neaktivní, což může mít za následek dočasnou nefunkčnost mapované služby.

- *Překládat port na* — při záměně cílové adresy může být zaměněn i port dané služby. Služba tedy může fyzicky běžet na jiném portu, než na kterém je dostupná z Internetu. *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.

Příklady nastavení komunikačních pravidel pro mapování portů naleznete v kapitole 7.4.

Záznam

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



Obrázek 7.19 Komunikační pravidlo — záznam paketů a/nebo spojení

- *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 (k vytvoření spojení nedojde).

Následující dva sloupce jsou ve výchozím nastavení okna *Komunikační pravidla* skryté (nastavení zobrazovaných sloupců viz kapitola 3.2):

Platí v

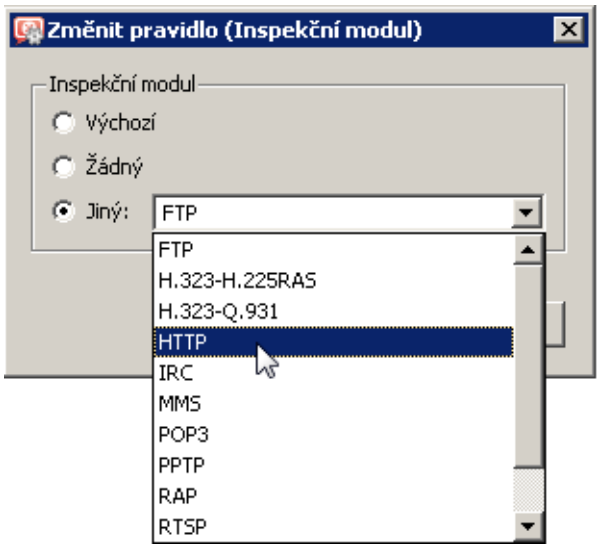
Časový interval, ve kterém má pravidlo platit. Mimo tento časový interval se *WinRoute* chová tak, jako by pravidlo neexistovalo.

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

V okamžiku začátku platnosti zakazujícího pravidla a v okamžiku skončení platnosti povolujícího pravidla jsou ihned ukončena všechna aktivní síťová spojení vyhovující příslušnému pravidlu.

Inspekční modul

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



Obrázek 7.20 Komunikační pravidlo — výběr inspekčního modulu

- *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 aplikován na komunikaci popsanou tímto pravidlem (k dispozici jsou všechny inspekční moduly, které *WinRoute* obsahuje). Na danou komunikaci nebude aplikován žádný další inspekční modul, bez ohledu na nastavení služeb v položce *Služba*.

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.
Další informace naleznete v kapitole 7.7.

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).

7.4 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 (NAT)

Překlad IP adres (též sdílení internetového připojení) znamená záměnu zdrojové (privátní) IP adresy v paketu jdoucím z lokální sítě do Internetu za IP adresu vnějšího rozhraní počítače s *WinRoute*. Tato technika se používá pro připojení lokální privátní sítě k Internetu prostřednictvím jedné veřejné IP adresy.

Příslušné komunikační pravidlo může vypadat následovně:

Jméno	Zdroj	Cíl	Služba	Akce	Překlad
NAT	Důvěryhodné / lokální	Internet	Libovolný	✓	NAT

Obrázek 7.21 Typické komunikační pravidlo pro překlad IP adres (sdílení internetového připojení)

Zdroj

Skupina rozhraní *Důvěryhodné / lokální*. Tato skupina obsahuje všechny segmenty lokální sítě připojené přímo k firewallu. Pokud nemá být z některých segmentů povolen přístup do Internetu, je nevhodnější zařadit příslušné rozhraní do skupiny *Ostatní rozhraní*.
Je-li lokální síť tvořena kaskádními segmenty (tzn. obsahuje další směrovače), není třeba to v pravidle zohledňovat — pouze je nutné správně nastavit směrování (viz kapitola 18.1).

Cíl

Skupina rozhraní *Internet*. S použitím této skupiny je pravidlo univerzálně použitelné pro libovolný typ internetového připojení (viz kapitola 6) a ani v případě změny internetového připojení není nutné pravidlo měnit.

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 *Výchozí nastavení* — pro NAT se použije primární IP adresa rozhraní, přes které paket odchází z počítače s *WinRoute*. Tím je rovněž zajištěna univerzálnost pravidla — překlad adres bude probíhat vždy správně, bez ohledu na typ internetového připojení a konkrétní linku, přes kterou bude paket odeslán do Internetu.

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 explicitně povolena samostatným pravidlem. Protože počítač s *WinRoute* má přímý přístup do Internetu, není nutné použít překlad IP adres.

Jméno	Zdroj	Cíl	Služba	Akce	Překlad
Komunikace firewallu	Firewall	Libovolný	Libovolný	✓	

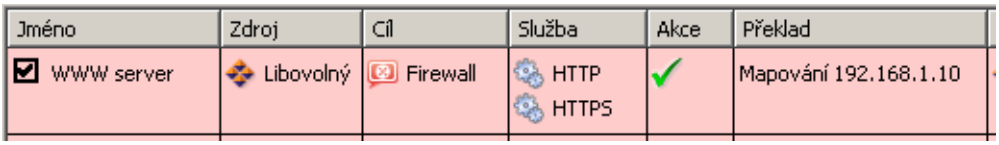
Obrázek 7.22 Pravidlo pro komunikaci firewallu s počítači v Internetu

Zpřístupnění služby (mapování portů)

Mapování portů zpřístupňuje z Internetu službu na počítači v lokální (zpravidla privátní) síti. Z pohledu klienta tato služba běží na vnější (veřejné) IP adrese počítače s *WinRoute*.

Od verze *6.4.0 WinRoute* umožňuje přístup k mapované službě také z lokální sítě. Odpadají tedy komplikace s různými DNS záznamy pro Internet a lokální síť.

Komunikační pravidlo pro mapování portů může být definováno následovně:



Obrázek 7.23 Komunikační pravidlo pro zpřístupnění lokálního WWW serveru z Internetu

Zdroj

K mapované službě se mohou připojovat klienti jak z Internetu, tak z lokální sítě. Z tohoto důvodu je možné v položce *Zdroj* ponechat hodnotu *Libovolný* (případně můžeme uvést všechny relevantní skupiny rozhraní nebo jednotlivá rozhraní — např. *Internet* a *LAN*).

Cíl

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

Takto bude služba přístupná na všech adresách rozhraní připojeného k Internetu. Chceme-li službu zpřístupnit na konkrétní IP adrese, použijeme volbu *Počítač* a zadáme požadovanou IP adresu (viz příklad pro multihoming).

Služba

Služby, které mají být zpřístupněny. Službu lze vybrat ze seznamu předdefinovaných služeb (viz kapitola 14.3) 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 z Internetu.

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

Jak již bylo zmíněno, k mapovaným službám je možné přistupovat i z lokální sítě. Při přístupu z lokální sítě se navazuje spojení z lokální (privátní) IP adresy na IP adresu v Internetu (veřejnou IP adresu firewallu). Pokud by pravidlu pro mapovanou službu předcházelo pravidlo povolující přístup z lokální sítě do Internetu, paket by na základě tohoto pravidla byl směrován do Internetu a následně zahozen. Z tohoto důvodu doporučujeme všechna pravidla pro mapované služby umisťovat vždy *na začátek* tabulky komunikačních pravidel.

Poznámka: Existují-li samostatná pravidla omezující přístup k mapovaným službám, musí být tato pravidla umístěna nad vlastními pravidly pro mapování. Zpravidla však lze mapování služby a omezení přístupu zkombinovat do jediného pravidla.

Zpřístupnění služeb na různých IP adresách (multihoming)

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

Předpokládejme, že 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 k 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:

Jméno	Zdroj	Cíl	Služba	Akce	Překlad
Mapování pro server Web1	Libovolný	95.13.184.10	HTTP	✓	Mapování 192.168.1.100
Mapování pro server Web2	Libovolný	95.13.184.11	HTTP	✓	Mapování 192.168.1.200

Obrázek 7.24 Multihoming — mapování WWW serverů

Zdroj
: Libovolný (viz předchozí příklad pro mapování jedné služby).

Cíl
: Příslušná IP adresa rozhraní připojeného k 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 odpovídajícího WWW serveru (`web1`, resp. `web2`).

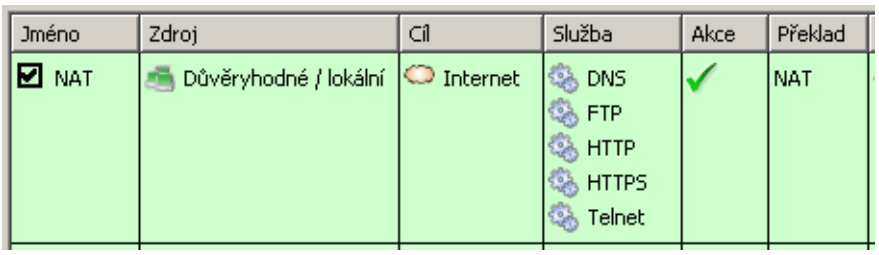
Omezení přístupu do Internetu

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).

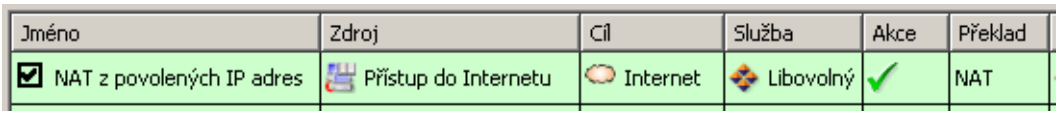
Poznámka: Pravidla uvedená v těchto příkladech mohou být také použita, jestliže je *WinRoute* nasazen jako tzv. neutrální směrovač (tj. směrovač bez překladu IP adres) — pouze v položce *Překlad* nebude žádný překlad definován.

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



Obrázek 7.25 Sdílení internetového připojení — povolení přístupu pouze k vybraným službám

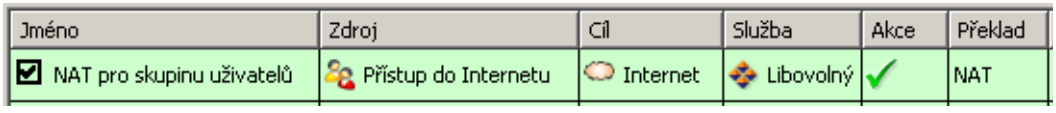
2. Omezení dle IP adres. Přístup k určitým službám (případně kompletní přístup do Internetu) bude povolen pouze z vybraných počítačů. V položce *Zdroj* definovaného pravidla uvedeme skupinu IP adres, ze kterých bude přístup do Internetu povolen. Tuto skupinu je třeba nejprve definovat v sekci *Konfigurace* → *Definice* → *Skupiny* (viz kapitola 15.5).



Obrázek 7.26 Povolení přístupu do Internetu pouze pro vybranou skupinu IP adres

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



Obrázek 7.27 Povolení přístupu do Internetu pouze vybrané skupině uživatelů

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 pak má detailní přehled o tom, kam kteří uživatelé přistupují a jaké služby využívají (anonymní přístup není možný).

Obrázek 7.28 Povolení přístupu do Internetu pouze ověřeným uživatelům

Podrobné informace o přihlašování uživatelů k firewallu naleznete v kapitole 10.1.

Poznámka:

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

2. Použití uživatelských účtů a skupin uživatelů v komunikačních pravidlech má určitá specifika. Touto problematikou se podrobně zabývá kapitola 7.6.

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 přístupu na servery v Internetu pomocí 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.

Obrázek 7.29 Výjimka — povolení služby Telnet pouze vybrané skupině uživatelů

7.5 Policy routing

Pokud je lokální síť připojena do Internetu více linkami s rozložením zátěže (viz kapitola 6.4), může vzniknout požadavek, aby pro určitou komunikaci byla vyhrazena jedna linka a ostatní komunikace byla směrována přes zbývající linky. Důvodem je, aby důležitá komunikace (např. e-mail nebo informační systém) nebyla zbytečně zpomalována méně důležitou komunikací (např. „brouzdání“ uživatelů po WWW stránkách či poslech internetových rádií). Pro splnění tohoto požadavku je potřeba při směrování paketů z lokální sítě do Internetu kromě cílové IP adresy pracovat také s dalšími informacemi — zdrojovou IP adresou, protokolem atd. Tato technika směrování se nazývá *policy routing* (inteligentní směrování).

Ve *WinRoute* lze policy routing definovat pomocí podmínek v komunikačních pravidlech pro přístup do Internetu s překladem IP adres (NAT). Tato koncepce nabízí velmi široké možnosti pro splnění všech požadavků na směrování a rozložení zátěže internetového připojení.

Poznámka: Komunikační pravidla pro *policy routing* mají vyšší prioritu než cesty definované ve směrovací tabulce (viz kapitola 18.1).

Příklad: Vyhrazená linka pro e-mailovou komunikaci

Předpokládejme, že firewall je připojen do Internetu dvěma linkami s rozložením zátěže o rychlostech *4 Mbit/s* a *8 Mbit/s*. První z linek je připojena k poskytovateli, u kterého je zároveň hostován poštovní server. Proto je požadováno, aby veškerá e-mailová komunikace (protokoly *SMTP*, *IMAP*, *POP3* a jejich zabezpečené verze) byla směrována touto linkou.

Pro splnění uvedených požadavků definujeme dvě komunikační pravidla:

- První pravidlo určuje, že pro e-mailové služby bude prováděn překlad IP adres (NAT) s použitím rozhraní *Internet 4 Mbit*.
- Druhé pravidlo je obecné pravidlo pro NAT s automatickým výběrem rozhraní (viz kapitola 7.4).

Jméno	Zdroj	Cíl	Služba	Akce	Překlad
NAT - vyhrazená linka pro e-mail	Důvěryhodné / lokální	Internet	IMAP IMAPS POP3 POP3S SMTP SMTPS	✓	NAT (Internet 4Mbit)
NAT - ostatní služby	Důvěryhodné / lokální	Internet	Libovolný	✓	NAT

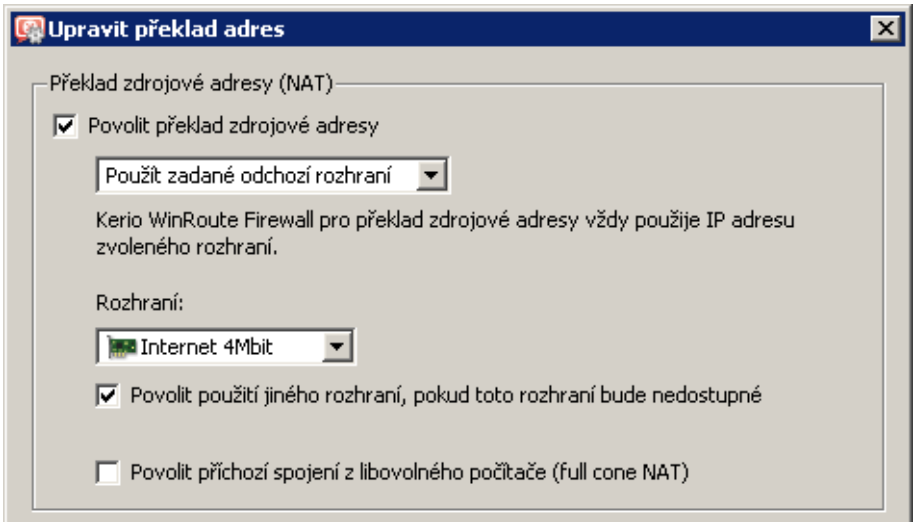
Obrázek 7.30 Policy routing — vyhrazená linka pro e-mail

Nastavení překladu IP adres v pravidle pro e-mailové služby je zřejmé z obrázku 7.31. Doporučujeme povolit použití jiné linky, pokud dojde výpadku vyhrazené linky. V opačném případě by po dobu výpadku vyhrazené linky byly e-mailové služby nedostupné.

Předpokládejme, že poštovní server poskytuje také služby *Webmail* a *CalDAV*, které používají protokol *HTTP(s)*. Přidání těchto protokolů do prvního pravidla by způsobilo, že by přes vyhrazenou linku byla směrována veškerá WWW komunikace. Pravidlo však můžeme modifikovat tak, aby linka byla vyhrazena pro komunikaci s konkrétním serverem — viz obrázek 7.32.

Poznámka: Ve druhém pravidle je použit automatický výběr rozhraní. To znamená, že i linka *Internet 4Mbit* bude stále využita pro rozložení zátěže internetového připojení. Přitom samozřejmě bude zohledňována e-mailová komunikace, pro kterou je linka vyhrazena podle prvního pravidla. Celková zátěž tak bude stále optimálně rozložena mezi obě linky.

Pokud bychom z nějakého důvodu požadovali, aby určitá linka byla vyhrazena *pouze* pro danou komunikaci a veškerá ostatní komunikace byla směrována přes jiné linky, pak v sekci



Obrázek 7.31 Policy routing — nastavení NAT pro vyhrazenou linku

Jméno	Zdroj	Cíl	Služba	Akce	Překlad
NAT - vyhrazená linka pro e-mail	Důvěryhodné / lokální	mail.server.cz	Libovolný	✓	NAT (Internet 4Mbit)
NAT - ostatní služby	Důvěryhodné / lokální	Internet	Libovolný	✓	NAT

Obrázek 7.32 Policy routing — vyhrazená linka pro konkrétní server

Konfigurace → *Rozhraní* nastavíme této lince rychlost *0 Mbit/s*. Linka pak nebude použita pro rozložení zátěže, ale bude přes ni směrována pouze specifická komunikace dle komunikačních pravidel.

Příklad: Optimalizace rozložení zátěže internetového připojení

WinRoute nabízí dva způsoby rozložení zátěže internetového připojení: podle zdrojových počítačů (klientů) nebo podle jednotlivých spojení (bližší informace viz kapitola 7.3). Vzhledem k různorodosti aplikací na jednotlivých počítačích a různým povahám uživatelů je zřejmé, že lepšího využití jednotlivých internetových linek se dosáhne při rozložení zátěže podle jednotlivých spojení. V tomto režimu však může docházet k problémům při přístupu ke službám, kde se navazuje více spojení současně (typicky WWW stránky a další služby založené na WWW). Server může různé zdrojové adresy v jednotlivých spojeních vyhodnotit jako obnovení spojení po výpadku (pak dojde např. k vypršení relace) nebo jako pokus o útok (služba pak může být zcela nedostupná).

Řešením tohoto problému je použít policy routing. Pro „problematické“ služby (např. *HTTP* a *HTTPS*) bude zátěž rozložena podle klientů, tzn. všechna spojení z jednoho klienta budou směrována přes jednu internetovou linku a budou tedy mít shodnou zdrojovou IP adresu. Na ostatní služby bude aplikováno rozložení zátěže podle spojení — tím bude zajištěno optimální využití kapacity jednotlivých linek.

Uvedené požadavky zajistí dvě komunikační pravidla pro NAT — viz obrázek 7.33. V prvním pravidle uvedeme požadované služby a nastavíme režim NAT *podle počítačů*. Druhé pravidlo bude platit pro libovolnou (jinou) službu a nastavíme zde režim NAT *podle spojení*.

Jméno	Zdroj	Cíl	Služba	Akce	Překlad
NAT - rozložení dle klientů	Důvěryhodné / lokální	Internet	HTTP HTTPS	✓	NAT
NAT - rozložení dle spojení	Důvěryhodné / lokální	Internet	Libovolný	✓	NAT Rozložení zátěže podle spojení

Obrázek 7.33 Policy routing — optimalizace rozložení zátěže

7.6 Použití uživatelských účtů a skupin v komunikačních pravidlech

V komunikačních pravidlech lze jako zdroj (případně cíl) použít také uživatelské účty a/nebo skupiny uživatelů. Uživatelský účet má v pravidle význam IP adresy počítače, ze kterého je uživatel přihlášen. Pravidlo se tedy uplatní pouze v případě, že je uživatel na firewallu ověřen (po odhlášení uživatele je pravidlo opět neplatné). V této kapitole popisujeme aspekty, které mohou vzniknout při použití uživatelských účtů v komunikačních pravidlech, a řešení těchto problémů.

Poznámka: Podrobné informace o definici komunikačních pravidel viz kapitola 7.3.

Povolení přístupu do Internetu vybraným uživatelům

Požadavkem je povolit přístup do Internetu (ke všem službám) pouze vybraným uživatelům. Předpokládejme, že se jedná o privátní lokální síť a přístup do Internetu je realizován pomocí technologie NAT. Pak stačí příslušné uživatele uvést v položce *Zdroj* pravidla pro překlad adres.

Jméno	Zdroj	Cíl	Služba	Akce	Překlad
NAT	jnovak kmasek mcerna	Internet	Libovolný	✓	NAT

Obrázek 7.34 Komunikační pravidlo povolující přístup do Internetu pouze vybraným uživatelům

Takto definované pravidlo povolí přístup do Internetu vyjmenovaným uživatelům, pokud budou na firewallu ověřeni. Tito uživatelé však budou muset ručně otevřít přihlašovací stránku WWW rozhraní *WinRoute* a přihlásit se (podrobnosti viz kapitola 10.1).

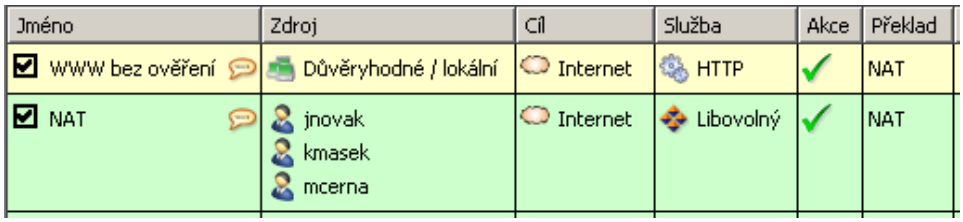
S takto definovaným pravidlem však budou neúčinné všechny metody automatického ověřování (tj. přesměrování na přihlašovací stránku, NTLM ověřování a automatické přihlášení z definovaných počítačů). Automatické ověření (resp. přesměrování na přihlašovací stránku) se totiž provádí až v okamžiku navazování spojení do Internetu (z důvodu sledování využití

licence — viz kapitola 4.6). Toto pravidlo pro překlad adres však nepovolí navázat spojení dříve, než je příslušný uživatel ověřen.

Povolení automatického ověřování

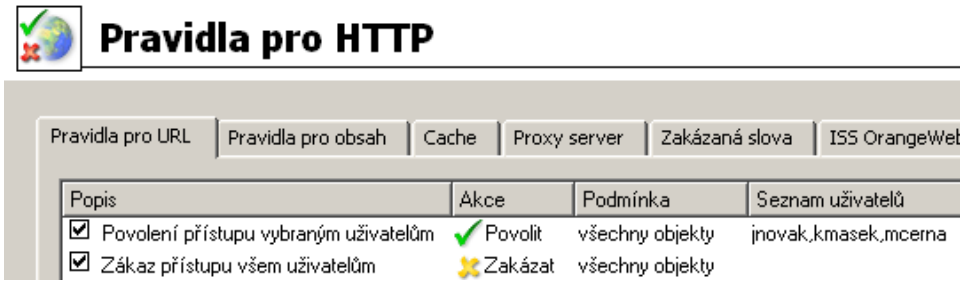
Problém s automatickým ověřováním uživatelů můžeme snadno vyřešit následujícím způsobem:

- Nad pravidlo pro překlad IP adres přidáme pravidlo povolující přístup ke službě *HTTP* bez omezení.



Obrázek 7.35 Komunikační pravidla umožňující automatické přesměrování na přihlašovací stránku

- V pravidlech pro URL (viz kapitola 12.2) povolíme přístup ke všem WWW stránkám vybraným uživatelům a zakážeme přístup všem ostatním uživatelům.



Obrázek 7.36 Pravidla pro URL umožňující přístup ke všem WWW stránkám pouze vybraným uživatelům

Pokud uživatel nebude dosud ověřen a pokusí se přistoupit na nějakou WWW stránku, bude automaticky přesměrován na přihlašovací stránku (příp. ověřen pomocí NTLM nebo automaticky přihlášen z příslušného počítače). Po úspěšném ověření bude uživatelům uvedeným v pravidle *NAT* (viz obrázek 7.35) povolen přístup i k ostatním službám v Internetu. Neověřeným uživatelům a ostatním uživatelům, kteří nejsou v pravidlech uvedeni, bude zakázán přístup na všechny WWW stránky a všechny ostatní služby v Internetu.

Poznámka: V tomto příkladu předpokládáme, že klientské počítače využívají *DNS forwarder* ve *WinRoute*, případně DNS server v lokální síti, jehož komunikace je povolena. Pokud by klientské stanice používaly přímo DNS server v Internetu (nedoporučená konfigurace!), musela by do pravidla povolujícího přístup bez omezení být přidána ještě služba *DNS*.

7.7 Vyřazení inspekčního modulu pro určitou službu

V některých případech nemusí být aplikování inspekčního modulu na danou komunikaci žádoucí. Pro vyřazení určitého inspekčního modulu je třeba definovat komunikační pravidlo pro tuto službu a odpovídající zdrojové a cílové adresy, ve kterém explicitně nastavíme, že nemá být používán žádný inspekční modul.

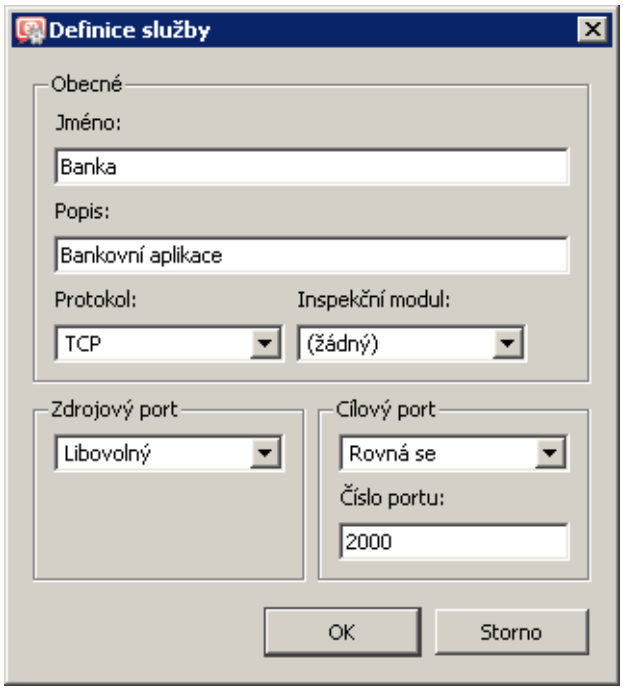
Příklad

Klient elektronického bankovnictví komunikuje se serverem banky vlastním aplikačním protokolem, který využívá transportní protokol TCP na portu 2000. Předpokládejme, že tato aplikace je provozována na počítači s IP adresou `192.168.1.15` a připojuje se k serveru `server.banka.cz`.

Port 2000 je standardně využíván protokolem *Cisco SCCP*. Za normálních okolností by byl na komunikaci bankovního klienta aplikován inspekční modul protokolu *SCCP*, což by mohlo způsobit nesprávnou funkci této aplikace, případně degradovat zabezpečení.

Pro komunikaci bankovního klienta definujeme speciální komunikační pravidlo:

1. V sekci *Konfigurace* → *Definice* → *Služby* definujeme službu *Banka*: služba využívá transportní protokol TCP na portu 2000 a nepoužívá žádný inspekční modul.



Obrázek 7.37 Definice služby bez inspekčního modulu

2. V sekci *Konfigurace* → *Komunikační pravidla* vytvoříme pravidlo povolující komunikaci této službě z počítače v lokální síti na server banky. V pravidle specifikujeme, že nemá být použit žádný inspekční modul.

Obrázek 7.38 Komunikační pravidlo povolující přístup ke službě bez inspekce protokolu

Poznámka: Ve výchozím nastavení sekce *Komunikační pravidla* je sloupec *Inspekční modul* skryt. K jeho zobrazení využijeme funkci *Nastavit sloupce* (viz kapitola 3.2).

Upozornění

K vyřazení inspekčního modulu pro určitou komunikaci nestačí definovat službu bez použití tohoto modulu! Inspekční moduly jsou aplikovány automaticky na veškerou komunikaci příslušnými protokoly. Vyřazení určitého inspekčního modulu musí být specifikováno komunikačními pravidly.

7.8 Použití Full cone NAT

Řada aplikací (zejména programy pro multimédia, internetovou telefonii (VoIP) apod.) používá model komunikace, kdy se k portu „otevřenému“ odchozím paketem mohou připojit další klienti pro navázání přímého spojení. Pro tyto případy *WinRoute* nabízí režim překladu adres označovaný jako *Full cone NAT*. V tomto režimu je k otevřenému portu povolen přístup z libovolné IP adresy a komunikace je vždy přesměrována na příslušného klienta v lokální síti.

Použití *Full cone NAT* představuje určité bezpečnostní riziko. S každým odchozím spojením navázaným v tomto režimu se otevírá potenciální cesta z Internetu do lokální sítě. Pro zachování dostatečné úrovně zabezpečení je proto nutné povolovat *Full cone NAT* pouze pro konkrétní klienty a služby. Pro ilustraci uvádíme příklad pro IP telefon s protokolem SIP.

Poznámka: Podrobnosti o definici komunikačních pravidel viz kapitola 7.3.

Příklad: SIP telefon v lokální síti

Předpokládejme, že v lokální síti bude provozován IP telefon, který se registruje na SIP server v Internetu. Pro snazší popis uveďme konkrétní údaje:

- IP adresa telefonu: `192.168.1.100`
- Veřejná IP adresa firewallu: `195.192.33.1`
- SIP server: `sip.server.cz`

Protože firewall provádí překlad IP adres, telefon se na SIP serveru registruje pod veřejnou IP adresou firewallu (`195.192.33.1`). Při volání z jiného telefonu na tento telefon bude navazováno spojení na IP adresu firewallu (`195.192.33.1`) a příslušný port. Za normálních okolností

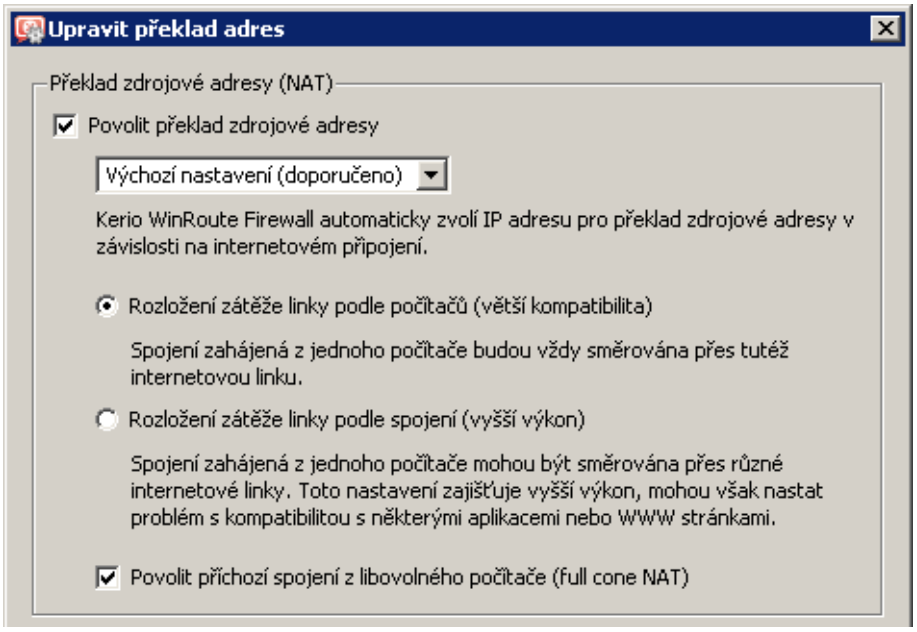
by takové spojení bylo možné navázat pouze přímo ze SIP serveru (na něj bylo navazováno původní odchozí spojení při registraci). Při použití *Full cone NAT* bude moci toto spojení navázat libovolný klient, který chce volat na SIP telefon v lokální síti.

Full cone NAT povolíme komunikačním pravidlem, které bude velmi restriktivní (z důvodu zachování maximální možné úrovně zabezpečení):

Jméno	Zdroj	Cíl	Služba	Akce	Překlad
Full Cone NAT	192.168.1.100	sip.server.cz	SIP	✓	Full cone NAT

Obrázek 7.39 Komunikační pravidlo pro Full cone NAT

- *Zdroj* — IP adresa SIP telefonu v lokální síti.
- *Cíl* — jméno nebo IP adresa SIP serveru v Internetu. *Full cone NAT* bude prováděn pouze pro komunikaci s tímto serverem.
- *Služba* — služba *SIP* (jedná se o SIP telefon). Pro ostatní služby nebude *Full cone NAT* prováděn.
- *Akce* — komunikace musí být povolena.
- *Překlad* — zvolíme požadovaný způsob překladu zdrojové IP adresy (viz kapitola 7.3) a zaškrtneme volbu *Povolit příchozí pakety z libovolné IP adresy (Full cone NAT).*



Obrázek 7.40 Povolení Full cone NAT v komunikačním pravidle

Pravidlo pro *Full cone NAT* musí být umístěno nad obecným pravidlem pro překlad adres povolujícím komunikaci z lokální sítě do Internetu.

7.9 Media hairpinning

WinRoute umožňuje „zprostředkovat“ komunikaci mezi dvěma klienty v lokální síti, kteří se vzájemně „znají“ pouze pod veřejnou IP adresou firewallu. Tato vlastnost firewallu se nazývá *hairpinning* (z angl. *hairpin* = serpentina, jedná se de facto o „otočení“ komunikace zpět do lokální sítě). Protože se využívá především při přenosu hlasových nebo obrazových dat, označuje se také jako *media hairpinning*.

Příklad: Dva SIP telefony v lokální síti

Předpokládejme situaci, kdy jsou v lokální síti umístěny dva SIP telefony. Tyto telefony se registrují na SIP serveru v Internetu. Pro snazší popis uveďme konkrétní údaje:

- IP adresy telefonů: `192.168.1.100` a `192.168.1.101`
- Veřejná IP adresa firewallu: `195.192.33.1`
- SIP server: `sip.server.cz`

Pro telefony definujeme příslušná komunikační pravidla — viz kapitola 7.8 (je zřejmé, že do položky *Zdroj* komunikačního pravidla pro *Full cone NAT* dle obrázku 7.39 stačí přidat IP adresu druhého telefonu).

Oba telefony budou zaregistrovány na SIP serveru pod veřejnou IP adresou firewallu (`195.192.33.1`). Uskuteční-li tyto telefony hovor mezi sebou, budou datové pakety (pro vlastní přenos hlasu) z každého telefonu posílány na veřejnou IP adresu firewallu (a port protějšího telefonu). Za normálních okolností by takové pakety byly zahazovány. *WinRoute* však dokáže na základě odpovídajícího záznamu v NAT tabulce rozpoznat, že paket je určen pro klienta v lokální síti, provede překlad cílové IP adresy a vyšle paket zpět do lokální sítě (stejně jako v případě mapování portů). Komunikace mezi oběma telefony tak bude fungovat správně.

Poznámka:

1. Podmínkou pro hairpinning je povolení příslušné komunikace mezi lokální sítí a Internetem (před zpracováním firewallem mají pakety zdrojovou adresu z lokální sítě a cílovou adresu z Internetu — jedná se tedy o odchozí komunikaci z lokální sítě do Internetu). Ve výchozích komunikačních pravidlech vytvořených průvodcem (viz kapitola 7.1) je tato podmínka splněna pravidlem *NAT*.

2. Hairpinning v principu nevyžaduje povolení *Full cone NAT* (viz kapitola 7.8). V uvedeném příkladu je však *Full cone NAT* nutný pro správnou funkci protokolu *SIP*.

Kapitola 8

Nastavení síťových služeb

Tato kapitola popisuje nastavení základních služeb, které *WinRoute* nabízí pro snadnou konfiguraci lokální sítě a přístupu do Internetu:

- Modul *DNS* — slouží jako jednoduchý DNS server pro lokální síť,
- *DHCP server* — zajišťuje plně automatickou konfiguraci počítačů v lokální síti,
- Klient služby *DDNS* — zajišťuje automatickou aktualizaci záznamů pro firewall ve veřejném dynamickém DNS,
- *Proxy server* — zajišťuje přístup do Internetu klientům, kteří nemohou nebo nechtějí využít přímý přístup,
- *HTTP cache* — urychluje přístup na opakovaně navštěvované WWW stránky (při přímém přístupu i při využití proxy serveru).

8.1 Modul DNS

Modul *DNS* slouží ve *WinRoute* ke zjednodušení konfigurace DNS na počítačích v lokální síti a pro zrychlení odpovědí na opakované DNS dotazy. DNS na lokálních počítačích lze 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. Všechny dotazy z každého počítače v lokální síti budou posílány do Internetu.
- 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 modul *DNS* ve *WinRoute*. Ten může sloužit jako jednoduchý DNS server pro lokální doménu a/nebo jako forwarder pro stávající DNS server.

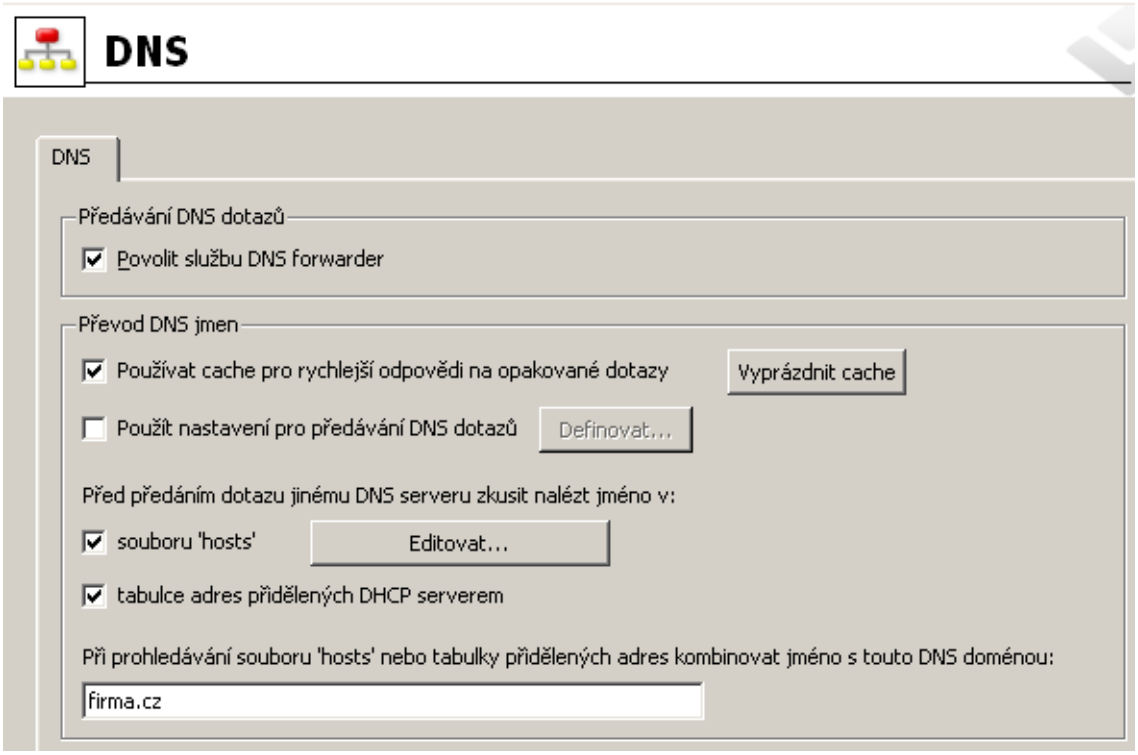
Je-li to možné, doporučujeme použít modul *DNS* jako primární DNS server pro počítače v lokální síti (poslední z uvedených možností). Tento modul zajistí rychlé zpracování DNS dotazů a jejich správné směrování ve složitějších síťových konfiguracích. Na opakované dotazy a dotazy na lokální DNS jména dokáže modul *DNS* odpovědět přímo, aniž by musel komunikovat s DNS servery v Internetu.

Pokud nedokáže modul *DNS* zodpovědět DNS dotaz sám, může jej předat na některý z DNS serverů nastavených na internetové lince, přes kterou je dotaz odesílán. Podrobnosti o konfiguraci síťových rozhraní firewallu naleznete v kapitole 5, bližší informace o možnostech internetového připojení v kapitole 6.

Konfigurace modulu DNS

Ve výchozím nastavení *WinRoute* je povolen DNS server (služba *DNS forwarder*), cache pro rychlejší odpovědi na opakované dotazy a jednoduchý převod DNS jmen.

Podrobnou konfiguraci lze provést v sekci *Konfigurace* → *DNS*.



Obrázek 8.1 Nastavení parametrů modulu DNS

Povolit službu DNS forwarder

Tato volba zapíná / vypíná DNS server ve *WinRoute*. Bez další konfigurace jsou všechny DNS dotazy předávány DNS serverům nastaveným na příslušném internetovém rozhraní. Je-li služba *DNS forwarder* vypnuta, slouží modul *DNS* pouze jako DNS resolver pro potřeby *WinRoute*.

Upozornění

Pokud ve vaší síťové konfiguraci nepoužijete *DNS forwarder*, můžete jej vypnout. Chcete-li na tomtéž počítači provozovat jiný DNS server, pak jej *musíte* vypnout — jinak by nastala kolize na portu služby DNS (`53/UDP`).

Používat cache pro rychlejší odpovědi

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

Fyzicky je DNS cache udržována v operační paměti, zároveň jsou však všechny DNS záznamy ukládány také do souboru `DnsCache.cfg` (viz kapitola 25.2). Díky tomu zůstávají

záznamy v DNS cache uchovány i při zastavení *WinRoute Firewall Engine*, resp. vypnutí firewallu.
Poznámka:

1. Doba uchování DNS záznamů v cache je specifikována přímo v každém záznamu (zpravidla 1 den).
2. Použití DNS cache zrychlí také činnost netransparentního proxy serveru ve *WinRoute* (viz kapitola 8.4).

Vyprázdnit cache
Smazání všech záznamů ve vyrovnávací paměti modulu *DNS* (bez ohledu na jejich dobu životnosti). Tuto funkci lze využít např. při změně konfigurace, při testování vytáčení na žádost, odhalování chyb apod.

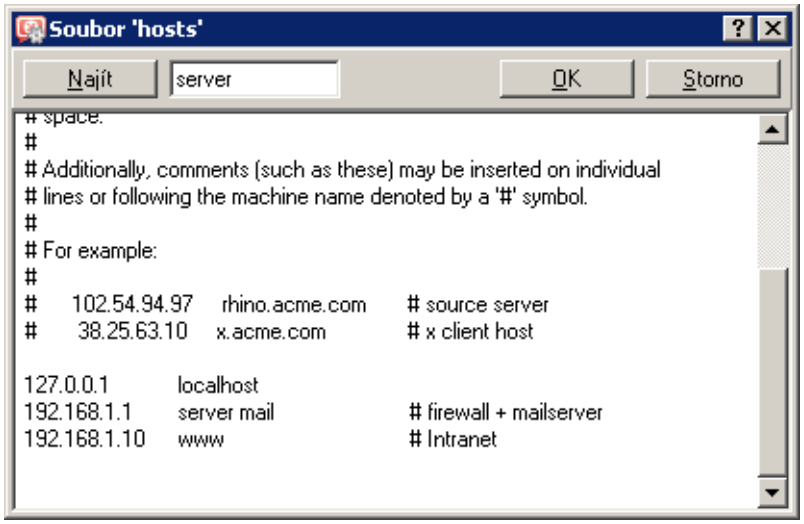
Použít nastavení pro předávání DNS dotazů
Tato volba aktivuje pravidla pro předávání DNS dotazů na jiné DNS servery (viz dále).

Jednoduchý převod DNS jmen

Modul *DNS* může určité DNS dotazy zodpovídat sám, typicky dotazy na jména počítačů v lokální síti. V lokální síti tak není potřeba žádný další DNS server ani není nutné ukládat informace o lokálních počítačích do veřejné DNS. Pro počítače konfigurované automaticky protokolem DHCP (viz kapitola 8.2) bude odpověď obsahovat vždy aktuální IP adresu.

Před předáním dotazu jinému DNS serveru...
Tyto volby umožňují nastavit, kde má modul *DNS* vyhledávat dotazované jméno (resp. IP adresu) předtím, než dotaz případně předá jinému DNS serveru.

- *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 modul *DNS*, je-li tato volba zapnuta. Tlačítko *Editovat* otevírá speciální editor, kterým lze soubor `hosts` upravovat přímo v *Administration Console*, a to i v případě, kdy je k *WinRoute* připojena vzdáleně (tj. z jiného počítače).
- *Tabulka adres přidělených DHCP serverem* — jsou-li počítače v lokální síti konfigurovány pomocí DHCP serveru ve *WinRoute* (viz kapitola 8.2), 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.
  Modul *DNS* 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. Tímto způsobem dochází de facto k dynamické aktualizaci DNS.



Obrázek 8.2 Editor systémového souboru hosts

Poznámka: Pokud jsou obě uvedené volby vypnuty, pak modul *DNS* předává všechny dotazy jiným DNS serverům.

Lokální DNS doména

Do pole *Při prohledávání souboru 'hosts' nebo tabulky přidělených adres kombinovat jméno s touto DNS doménou* je třeba zadat jméno lokální DNS domény.

Jestliže počítač nebo síťové zařízení vysílá požadavek na přidělení IP adresy, vkládá do něj pouze své jméno (doménu v tomto okamžiku ještě nezná). V tabulce adres přidělených DHCP serverem jsou proto uložena pouze jména počítačů bez domény. Aby modul *DNS* dokázal správně zodpovídat dotazy na plně kvalifikovaná lokální DNS jména (tj. jména včetně domény), musí znát jméno lokální domény.

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

Pro snazší pochopení uveďme jednoduchý příklad.

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 modul *DNS* neznal jméno lokální domény, předal by tento dotaz na jiný DNS server (dle nastavení — viz výše), protože by nerozpoznal, že se jedná o lokální počítač. Takto však může lokální doménu `firma.cz` oddělit a jméno `honza` s příslušnou IP adresou nalezne v tabulce DHCP serveru.

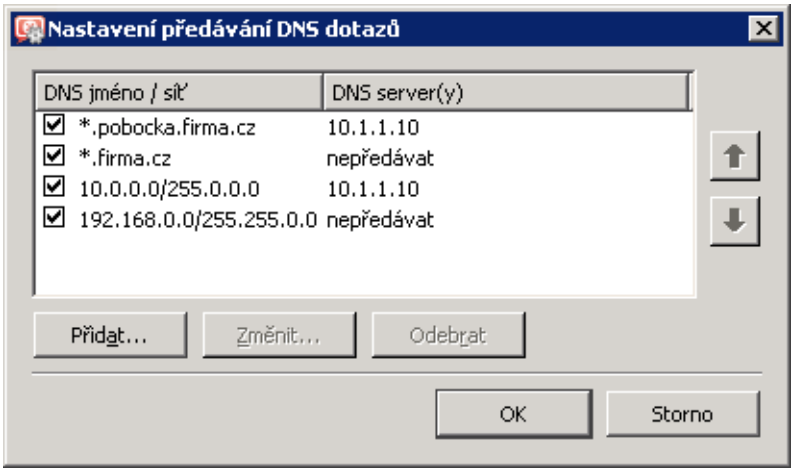
Nastavení předávání DNS dotazů

Modul *DNS* umožňuje předávat určité DNS dotazy na specifické DNS servery. Tuto funkci lze využít např. v případě, chceme-li pro lokální doménu používat DNS server v lokální síti (ostatní DNS dotazy budou předávány přímo do Internetu, čímž se zrychlí odezva). Nastavení předávání DNS dotazů je rovněž důležité při konfiguraci virtuálních privátních sítí, kdy je potřeba zajistit správné předání dotazů na jména v doménách vzdálených subsítí (podrobnosti viz kapitola 23).

Předávání dotazů se definuje pravidly pro DNS jména nebo subsítě. Pravidla tvoří uspořádaný seznam, který je vždy procházen shora dolů. Pokud DNS jméno nebo subsíť v dotazu vyhovuje některému pravidlu, pak bude tento dotaz předán na specifický DNS server a vyhodnocování pravidel se ukončí. Dotazy, které nevyhovují žádnému pravidlu, jsou předávány na „výchozí“ DNS servery (viz výše).

Poznámka: Je-li aktivní *Jednoduchý převod DNS jmen* (viz dále), pak se pravidla pro předávání dotazů uplatní pouze v případě, že modul *DNS* nedokáže dotaz zodpovědět na základě informací ze systémového souboru *hosts* a/nebo tabulky přidělených adres DHCP serveru.

Tlačítko *Definovat* v konfiguraci modulu *DNS* (viz obrázek 8.1) otevírá dialog pro nastavení pravidel pro předávání DNS dotazů.



Obrázek 8.3 Specifická nastavení předávání DNS dotazů

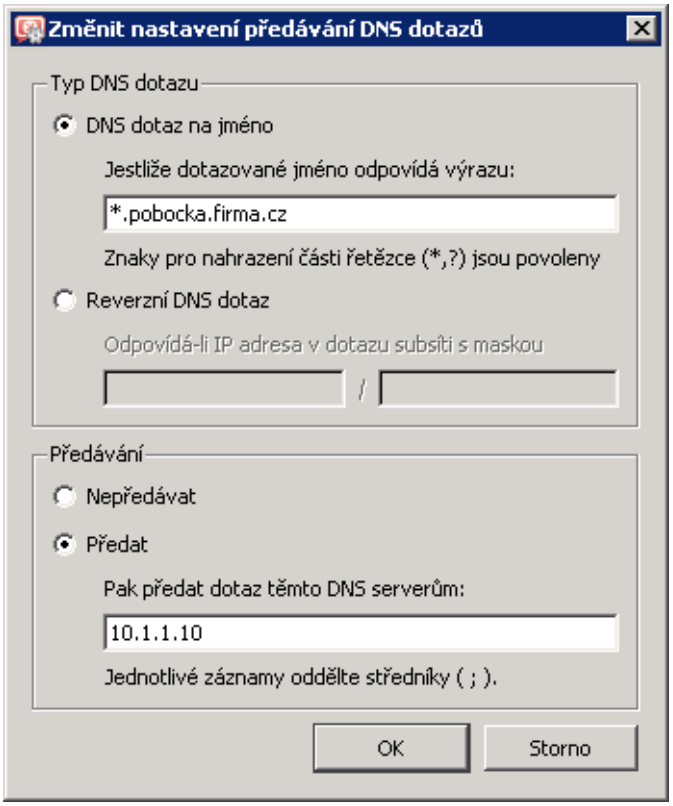
Pravidlo lze definovat pro:

- DNS jméno — pak budou na tento DNS server předávány dotazy na odpovídající jména počítačů (dotazy typu A)
- subsíť — pak budou na tento DNS server předávány dotazy na IP adresy v příslušné subsíti (reverzní doména — dotazy typu PTR)

Pořadí pravidel v seznamu je možné upravit tlačítky se šipkami v pravé části dialogu. Takto je možné vytvářet složitější kombinace pravidel — např. výjimky pro konkrétní počítače nebo subdomény. Protože je seznam pravidel procházen shora dolů, měla by být pravidla seřazena od nejspecifičtějšího (např. jméno konkrétního počítače) k nejobecnějšímu (např. hlavní doména firmy). Podobně pravidla pro reverzní DNS dotazy by měla být seřazena podle délky

masky subsítě (např. od `255.255.255.0` k `255.0.0.0`). Pravidla pro dotazy na jména a pro reverzní dotazy jsou vzájemně nezávislá. Pro přehlednost doporučujeme nejprve uvést všechna pravidla pro dotazy na jména a pak všechna pravidla pro reverzní dotazy, případně naopak.

Tlačítko *Přidat*, resp. *Změnit* otevírá dialog pro definici pravidla pro předávání DNS dotazů.



Obrázek 8.4 Předávání DNS dotazů — nové pravidlo

- Volba *DNS dotaz na jméno* slouží ke specifikaci pravidla pro dotazy na jména. Do pole *Jestliže dotazované jméno odpovídá výrazu* je třeba zadat příslušné DNS jméno (počítač v dané doméně).
  Ve většině případů nechceme předávat dotazy na konkrétní jména, ale pro celé domény. Proto může zadané jméno obsahovat zástupné znaky * (hvězdička — nahrazení libovolného počtu znaků) a ? (otazník — nahrazení právě jednoho znaku). Pravidlo pak bude platit pro všechna jména vyhovující zadanému řetězci (počítače, domény atd.).

  Příklad:

  DNS jméno zadáme ve tvaru: `*.?erio.c*`. Pravidlo bude platit pro všechna jména v doménách `kerio.cz`, `cerio.com`, `aerio.c` apod., tedy např. `www.kerio.cz`, `secure.kerio.com`, `www.aerio.c` atd.

Upozornění

V pravidlech pro DNS dotazy na jména je nutné vždy uvést výraz, kterému bude odpovídat celé DNS jméno! Pokud bychom zadali např. `kerio.c*`, pak by tomuto pravidlu vyhověla pouze jména `kerio.cz`, `kerio.com` apod., nikoliv však jména počítačů v těchto doménách (např. `www.kerio.cz` nebo `secure.kerio.com`)!

- Volba *Reverzní DNS dotaz* slouží ke specifikaci pravidla pro DNS dotazy na IP adresy v dané subsíti. Subsíť se zadává adresou sítě s příslušnou maskou (např. `192.168.1.0 / 255.255.255.0`).
- Do pole *Pak předat dotaz těmto DNS serverům* lze zadat IP adresu jednoho nebo více DNS serverů, na který mají být dotazy předávány.
  Je-li zadáno více DNS serverů, považují se za primární, sekundární atd.
  Volba *Nepředávat* znamená, že dotaz nebude předáván žádnému dalšímu DNS serveru — *WinRoute* bude pouze prohledávat lokální soubor `hosts`, příp. tabulky DHCP serveru (viz dále). Pokud zde dotazované jméno, resp. IP adresu nenalezne, odpoví klientovi, že toto jméno/adresa neexistuje.

8.2 DHCP server

DHCP (*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.).

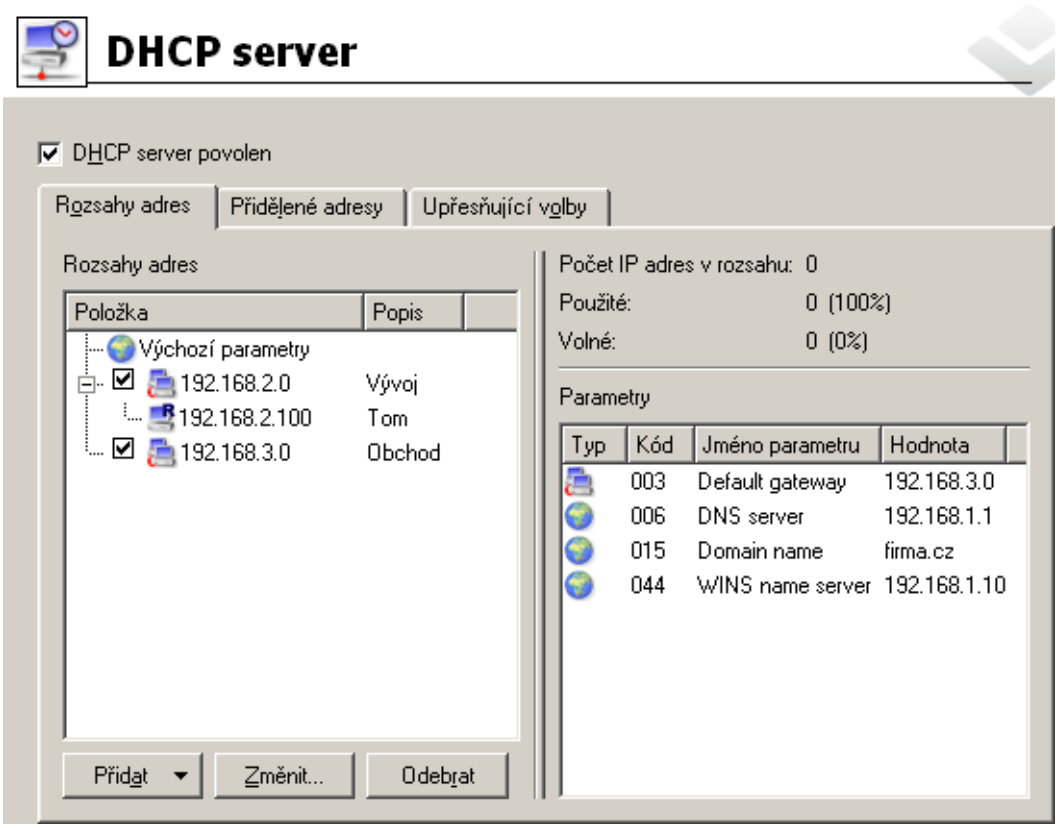
Konfigurace DHCP serveru

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

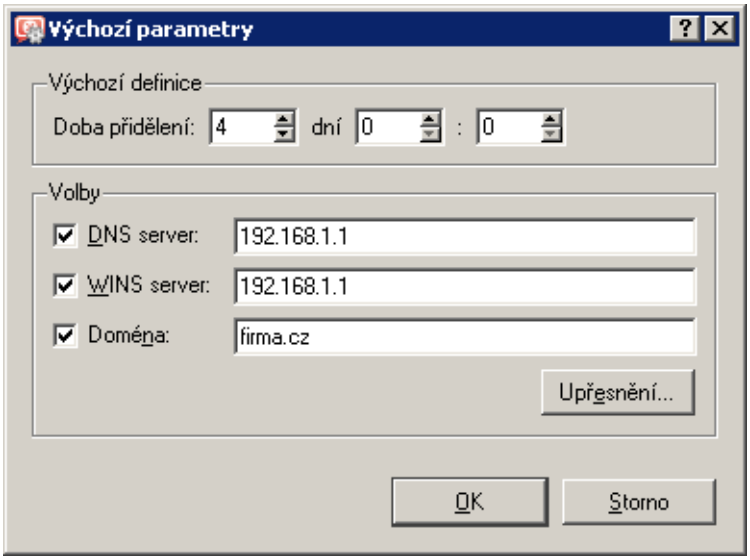
K definici rozsahů IP adres včetně volitelných parametrů slouží záložka *Rozsahy adres*. Záložka je rozdělena na dvě části, z nichž první obsahuje rozsahy adres a rezervace:



Obrázek 8.5 DHCP server — rozsahy přidělovaných IP adres

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.



Obrázek 8.6 DHCP server — výchozí DHCP parametry

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 modul *DNS* ve *WinRoute* (tj. IP adresu počítače s *WinRoute*). Modul *DNS* totiž dokáže spolupracovat s DHCP serverem (viz kapitola 8.1) a na dotazy na jména lokálních počítačů bude vždy odpovídat správnou IP adresou.

WINS server
: IP adresa WINS serveru.

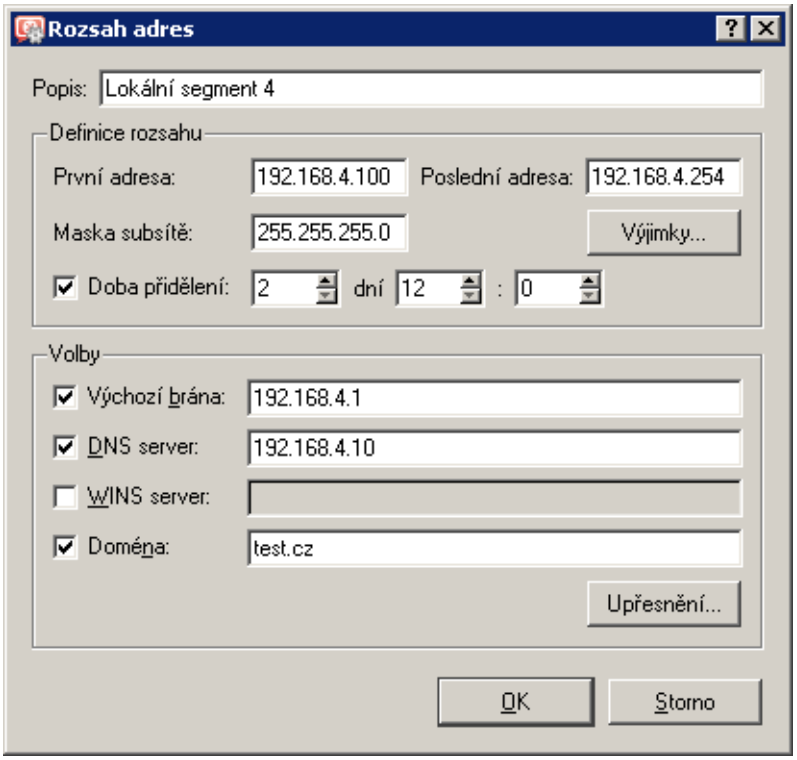
Doména
: Lokální internetová doména. Pokud lokální doména neexistuje, pak tento parametr nenastavujte.

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.



Obrázek 8.7 DHCP server — definice rozsahu 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 *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.

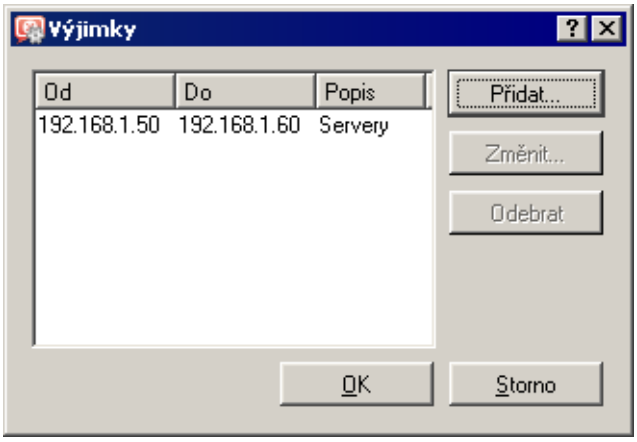
Výjimky

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.



Obrázek 8.8 DHCP server — výjimky z definovaného rozsahu adres

Parametry

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

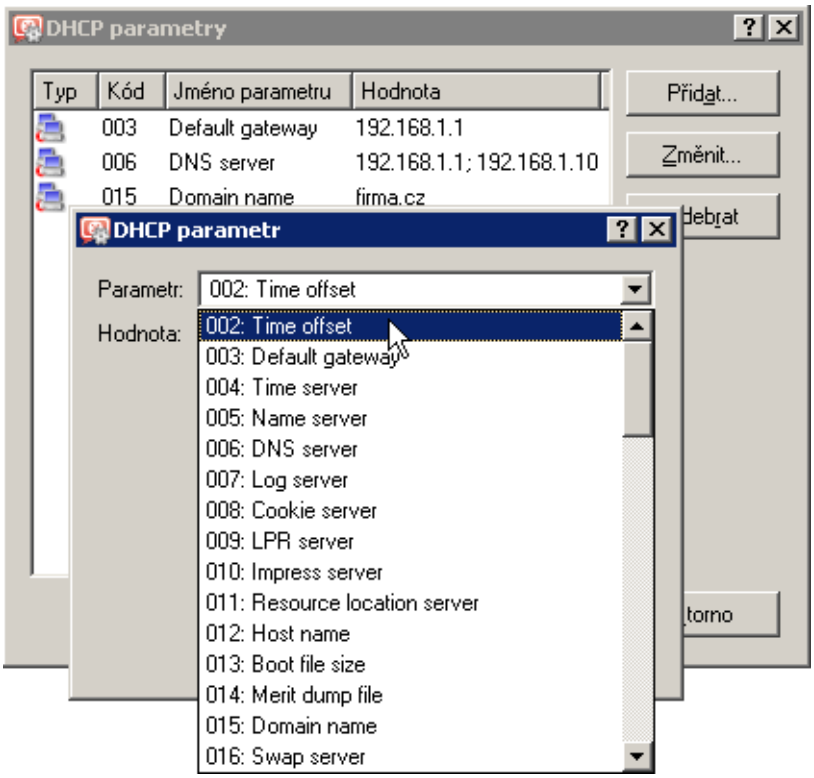
- *Výchozí brána* — musí být uvedena IP adresa směrovače, který je výchozí branou pro subsíť, z níž jsou IP adresy přidělovány (tzn. IP adresa rozhraní, ke kterému je daná subsíť připojena)! Výchozí brána v jiné subsíti nemá žádný smysl (byla by pro klienty nedosažitelná).
- *DNS server* — může být uveden libovolný DNS server (případně více DNS serverů oddělených středníky). Jako primární DNS server (tj. na prvním místě) však doporučujeme uvádět modul *DNS* ve *WinRoute* (tj. IP adresu počítače s *WinRoute*). Modul *DNS* totiž dokáže spolupracovat s DHCP serverem (viz kapitola 8.1) 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 domény *Windows NT*!

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*.



Obrázek 8.9 DHCP server — nastavení DHCP parametrů

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:

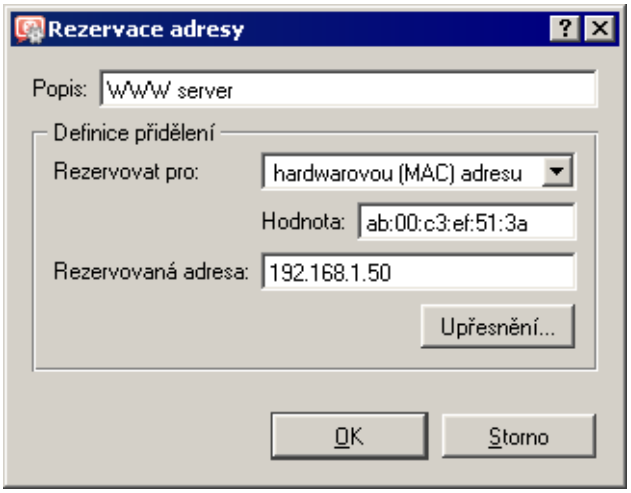
- celkový počet IP adres v tomto rozsahu
- počet a procentuální podíl přidělených adres
- počet a procentuální podíl volných adres

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

Obrázek 8.10 DHCP server — statistika (přidělené a volné adresy v rozsahu)

Rezervace IP adresy

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



Obrázek 8.11 DHCP server — rezervace IP adresy

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:

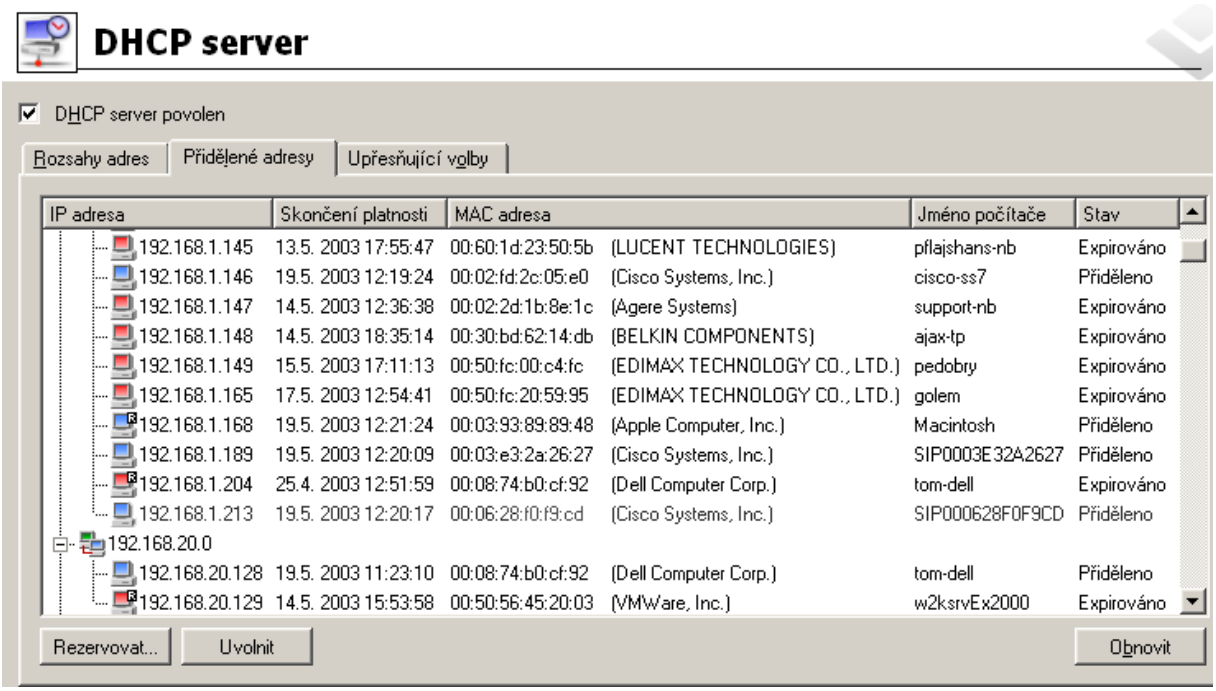
- hardwarovou (MAC) adresu počítače — zadává se v podobě hexadecimálních (šestnáctkových) čísel oddělených dvojtečkami — např.:
  `00:bc:a5:f2:1e:50`
  nebo pomlčkami — např.:
  `00-bc-a5-f2-1e-50`
  MAC adresu síťového adaptéru je možné zjistit pomocí nástrojů operačního systému (např. příkaz `ipconfig`), 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.



Obrázek 8.12 DHCP server — přehled přidělených a rezervovaných adres

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).
  Poznámka:
  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 vol-

ných 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 (nastavení zobrazovaných sloupců viz kapitola 3.2):

- *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.

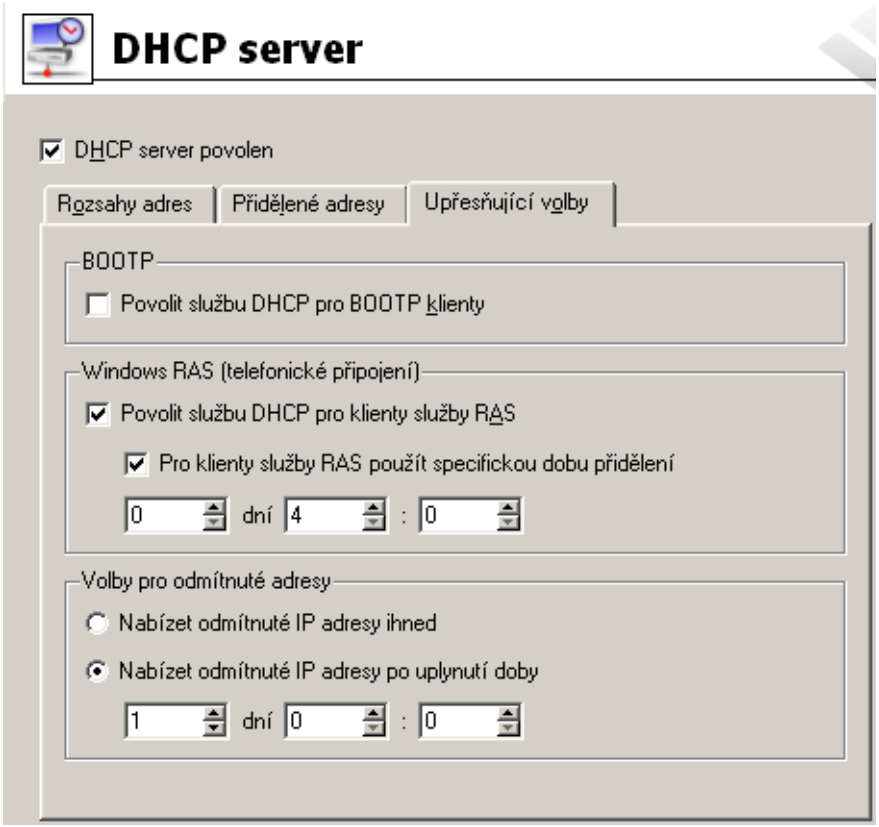
Poznámka: Do dialogu pro rezervaci IP adresy je automaticky dosazena MAC adresa počítače, kterému je daná IP adresa přidělena. Chcete-li IP adresu rezervovat pro jméno počítače, změňte nastavení položek *Rezervovat pro* a *Hodnota*.

Upřesňující volby pro DHCP server

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



Obrázek 8.13 DHCP server — upřesňující volby

Upozornění

1. DHCP server nemůže přidělovat adresy RAS klientům připojujícím se k RAS serveru přímo na počítači s *WinRoute* (z technických důvodů nelze přijímat DHCP požadavky z lokálního RAS serveru). V takovém případě je nutné nastavit přidělování IP adres přímo v konfiguraci RAS serveru.
2. Služba RAS ve *Windows* přiděluje při každém připojení novou IP adresu (i v případě, že se jedná o téhož klienta). *WinRoute* zahrnuje klienty služby RAS do celkového počtu klientů při kontrole, zda nedošlo k překročení počtu uživatelů povoleného licencí (viz kapitola 4.6). Z toho vyplývá, že za určitých podmínek (příliš velký rozsah IP adres pro službu RAS a/nebo příliš dlouhá doba přidělení adresy klientům RAS) může opakovaným připojováním RAS klientů dojít k překročení povoleného počtu uživatelů. Vzdálený klient se pak bude moci připojit a komunikovat s počítači v lokální síti, nebude však moci přistupovat přes *WinRoute* do Internetu.

Volby pro odmítnuté adresy

Nastavení v této sekci určuje, jakým způsobem budou použity 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*).

8.3 Dynamický DNS pro veřejnou IP adresu firewallu

Kerio WinRoute Firewall poskytuje (mimo jiné) služby pro vzdálený přístup do lokální sítě z Internetu (*VPN server* — viz kapitola 23 a rozhraní *Clientless SSL-VPN* — viz kapitola 24). Z Internetu mohou být přístupné i další služby — např. rozhraní *Kerio StaR* (viz kapitola 21), vzdálená správa *WinRoute* programem *Administration Console* (viz kapitola 16.2) nebo libovolná jiná služba (např. WWW server v lokální síti — viz kapitola 7.4). Tyto služby jsou dostupné na veřejné IP adrese firewallu. Pokud je tato IP adresa statická a existuje pro ni odpovídající DNS záznam, můžeme při přístupu k dané službě použít příslušné jméno počítače (např. `server.firma.cz`). Neexistuje-li DNS záznam, pak je nutné si zapamatovat IP adresu firewallu, a ke všem službám přistupovat pomocí IP adresy. Je-li navíc veřejná IP adresa dynamická (tzn. během času se mění), pak je velmi obtížné nebo téměř nemožné se k těmto službám z Internetu připojit.

Tento problém řeší podpora dynamického DNS ve *WinRoute*. Dynamický DNS zajistí DNS záznam pro vybrané jméno serveru, který bude vždy obsahovat aktuální IP adresu. Mapované služby tak budou vždy dostupné pod stejným jménem serveru, bez ohledu na to, zda a jak často se mění IP adresa.

Jak funguje spolupráce s dynamickým DNS?

Dynamický DNS (*DDNS*) je služba, která zajišťuje automatickou aktualizaci IP adresy v DNS záznamu pro dané jméno počítače. Služba DDNS je typicky nabízena ve dvou variantách:

- zdarma — uživatel si může vybrat z několika nabízených domén druhé úrovně (např. `no-ip.org`, `ddns.info` apod.) a vybrané doméně zvolit jméno počítače, které je dosud volné (např. `firma.ddns.info`).
- placená služba — uživatel si zaregistruje vlastní doménu (např. `firma.cz`) a poskytovatel služby pak zajišťuje DNS server pro tuto doménu s možností automatické aktualizace záznamů.

Uživateli služby DDNS je zřízen účet, který slouží k ověření přístupu, aby mohla aktualizaci DNS záznamů provádět pouze oprávněná osoba. Aktualizace navíc probíhá zabezpečeným spojením (typicky HTTPS), aby nebylo možné komunikaci odposlouchávat. Aktualizaci dynamických DNS záznamů může provádět buď přímo uživatel ručně nebo (častěji) specializovaný software — v tomto případě *WinRoute*.

Je-li *WinRoute* nastaven pro spolupráci s dynamickým DNS, pak při každé změně IP adresy internetového rozhraní (včetně přepnutí primárního / záložního internetového připojení — viz kapitola 6.3) vyšle požadavek na aktualizaci IP adresy v dynamickém DNS. Díky tomu je DNS záznam pro danou IP adresu stále aktuální a k mapovaným službám lze přistupovat pomocí daného jména počítače.

Poznámka:

1. Používání služby DDNS se řídí podmínkami konkrétního poskytovatele.

2. Dynamické DNS záznamy mají nastavenou velmi krátkou dobu životnosti (TTL), a proto jsou uchovávány v cache jiných DNS serverů nebo forwarderů po velmi krátkou dobu.

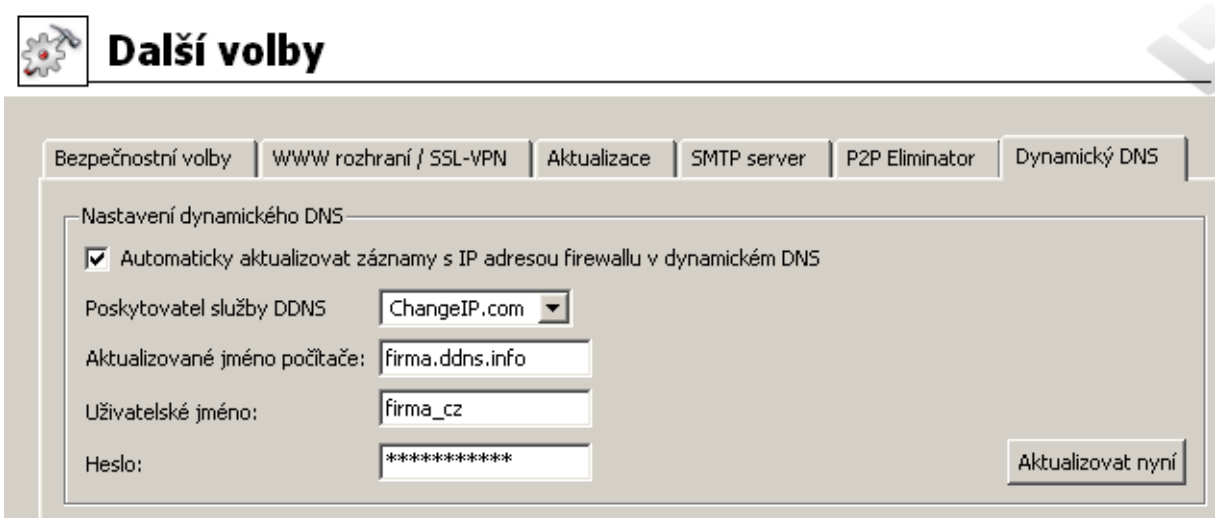
Pravděpodobnost, že klient dostane DNS odpověď s neplatnou (starou) IP adresou, je zcela minimální.

3. Některé DDNS servery umožňují také aktualizaci více záznamů současně. K tomuto účelu se používají zástupné znaky (wildcards).

   Příklad: V DDNS existují dvě jména počítačů, která obě odkazují na veřejnou IP adresu firewallu: `fw.firma.cz` a `server.firma.cz`. Při změně IP adresy stačí vyslat jeden požadavek na aktualizaci DNS záznamů se jménem `*.firma.cz`. Na základě tohoto požadavku budou aktualizovány DNS záznamy pro obě výše uvedená jména.

Konfigurace DDNS ve WinRoute

Spolupráci s dynamickým DNS serverem lze nastavit v sekci *Konfigurace / Další volby*, záložka *Dynamický DNS*.



Obrázek 8.14 Nastavení spolupráce s dynamickým DNS serverem

Jak již bylo zmíněno, nejprve je potřeba si zřídit účet (tzn. požadovaný dynamický DNS záznam s příslušnými přístupovými právy) u některého poskytovatele služby DDNS. *WinRoute* v současné době podporuje tyto poskytovatele DDNS:

- *ChangeIP* (http://www.changeip.com/),
- *DynDNS* (http://www.dyndns.org/),
- *No-IP* (http://www.no-ip.com/).

V záložce *Dynamický DNS* je třeba zvolit příslušného poskytovatele služby DDNS, zadat DNS jméno, pro které má být aktualizován dynamický záznam, a uživatelské jméno a heslo pro přístup k aktualizaci dynamického záznamu. Pokud DDNS server podporuje zástupné znaky (wildcards), můžeme je ve jméně počítače použít.

Po zadání všech údajů je doporučeno vyzkoušet aktualizaci dynamického DNS záznamu stisknutím tlačítka *Aktualizovat nyní*. Tím jednak ověříme, zda je automatická aktualizace funkční

(server je dostupný, zadané údaje jsou správné atd.), a zároveň zajistíme aktualizaci příslušného DNS záznamu (IP adresa firewallu se od registrace nebo poslední ruční aktualizace již mohla změnit).

Pokud při pokusu o aktualizaci DNS záznamu dojde k chybě, zobrazí se v záložce *Dynamický DNS* chybové hlášení s přesnou specifikací chyby (např. DDNS server není dostupný, selhalo ověření uživatele apod). Toto hlášení se rovněž zapíše do záznamu *error*.

8.4 Proxy server

WinRoute obsahuje klasický HTTP proxy server, přestože umožňuje díky technologii NAT přímý přístup do Internetu ze všech počítačů v lokální síti. V některých případech totiž 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 k Internetu je realizováno vytáčenou linkou a přístup na určité WWW stránky je blokován (viz kapitola 12.2). 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.

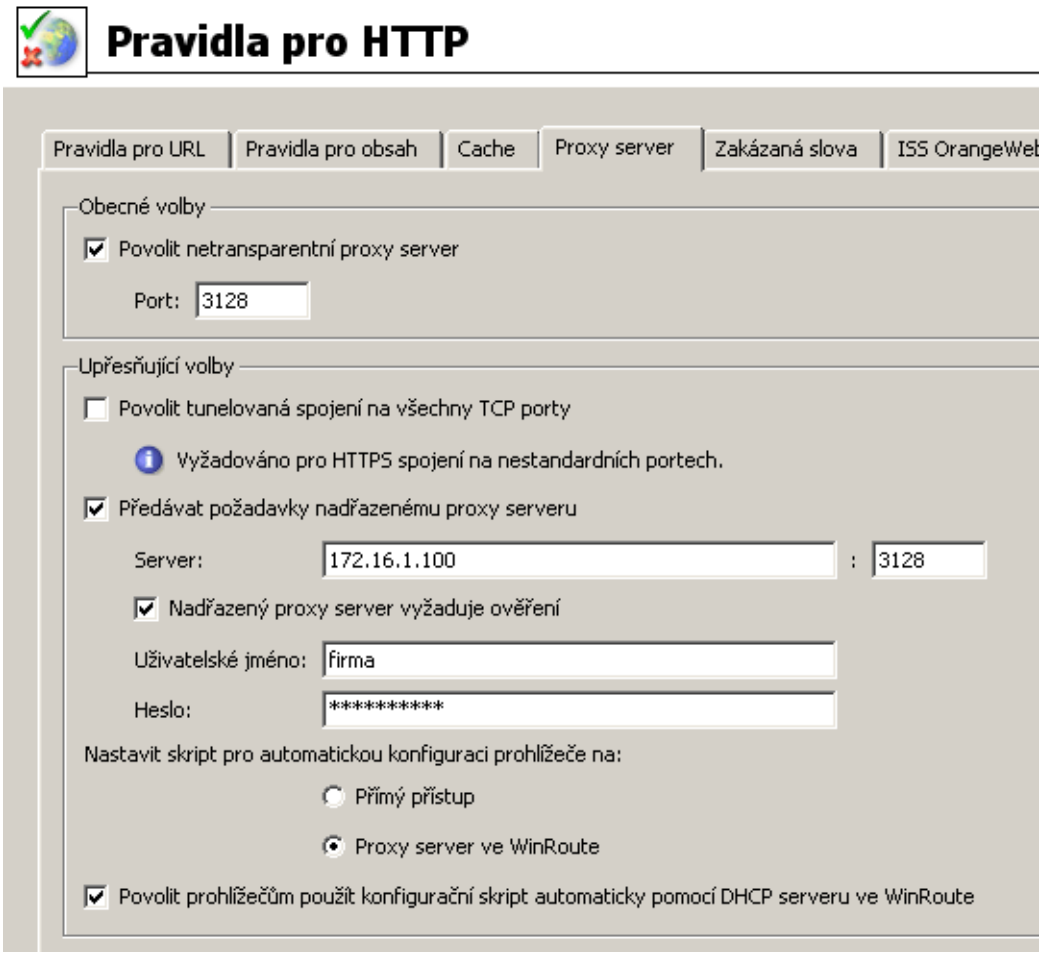
   Při použití proxy serveru zůstává přístup do Internetu funkční — konfigurace jednotlivých počítačů může zůstat nezměněna (případně lze změnit nastavení pouze na některých počítačích).

Proxy server ve *WinRoute* lze použít pro protokoly HTTP, HTTPS a FTP. Proxy server nepodporuje protokol SOCKS (speciální protokol pro komunikaci mezi klientem a proxy serverem).

Poznámka: Podrobné informace o použití FTP přes proxy server ve *WinRoute* naleznete v kapitole 25.4.

Konfigurace proxy serveru

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



Obrázek 8.15 Nastavení parametrů HTTP proxy serveru

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 22.8) se vypíše chybové hlášení v tomto tvaru:

```
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.

Povolit spojení na libovolný TCP port

Tato bezpečnostní volba umožňuje povolit nebo blokovat tzv. tunelování jiných aplikačních protokolů (než HTTP, HTTPS a FTP) přes proxy server.

Je-li tato volba vypnuta, pak proxy server povoluje navázání spojení pouze na standardní port služby HTTPS (`443`) — předpokládá se, že v tomto případě se jedná o přístup na zabezpečené WWW stránky. Je-li volba zapnuta, pak proxy server může navázat spojení na libovolný port. Může se jednat o protokol HTTPS na nestandardním portu, ale také o tunelování jiného aplikačního protokolu.

Poznámka: Na nezabezpečenou komunikaci protokoly HTTP a FTP nemá tato volba žádný vliv. HTTP a FTP komunikace je ve *WinRoute* obsluhována inspekčními moduly, které propustí pouze platné HTTP a FTP požadavky.

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`).
- *Nadřazený proxy server vyžaduje ověření* — tuto volbu zapněte, pokud nadřazený proxy server vyžaduje ověření uživatele jménem a heslem. Do položek *Uživatelské jméno* a *Heslo* vyplňte příslušné přihlašovací údaje.
  Poznámka: Jméno a heslo pro ověření na nadřazeném proxy serveru se posílá s každým HTTP požadavkem. Je podporováno pouze ověřování typu *Basic*.

Volba *Předávat požadavky nadřazenému proxy serveru* zároveň automaticky nastavuje způsob přístupu *WinRoute* do Internetu (pro kontrolu a stahování nových verzí, aktualizaci antiviru *McAfee* a přístup do online databází modulu *Kerio Web Filter*).

Nastavit skript pro automatickou konfiguraci ...

Pro použití proxy serveru je nutné správně nastavit parametry WWW prohlížečů na klientských počítačích. Většina současných prohlížečů (např. *Internet Explorer*, *Firefox/SeaMonkey*, *Opera* apod.) umožňuje automatickou konfiguraci skriptem staženým ze zadaného URL.

V případě proxy serveru ve *WinRoute* je konfigurační skript uložen na adrese:

```
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 prohlížečů* umožňuje přizpůsobit konfigurační skript tak, aby nastavoval prohlížeče správně podle aktuální konfigurace *WinRoute* a lokální sítě:

- *Přímý přístup* — v prohlížeči nebude nastaven žádný proxy server.
- *Proxy server ve WinRoute* — v prohlížeči bude nastavena IP adresa počítače s *WinRoute* a port, na kterém je proxy server spuštěn (viz výše).

Poznámka: Pro použití konfiguračního skriptu musí být proxy server vždy spuštěn (i v případě, že prohlížeče budou nastavovány pro přímý přístup).

Povolit prohlížečům použít konfigurační skript automaticky ...

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

Podmínkou použití této funkce je spuštěný DHCP server ve *WinRoute* (viz kapitola 8.2). Parametry TCP/IP na příslušné stanici však mohou být nastaveny staticky — *Internet Explorer* vyšle při svém spuštění speciální DHCP požadavek.

Tip

Tato volba umožňuje jediným kliknutím nastavit všechny prohlížeče *Internet Explorer* na počítačích v lokální síti.

8.5 HTTP cache

Cache slouží ke zrychlení přístupu na opakovaně navštěvované WWW stránky a snížení zatížení internetového připojení (v případě měřené linky je rovněž významné, že použití cache snižuje celkový 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. Ve výchozí konfiguraci *WinRoute* je tato podmínka splněna pro protokol HTTP na standardním portu 80 (podrobnosti viz kapitoly 7.3 a 14.3).

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).

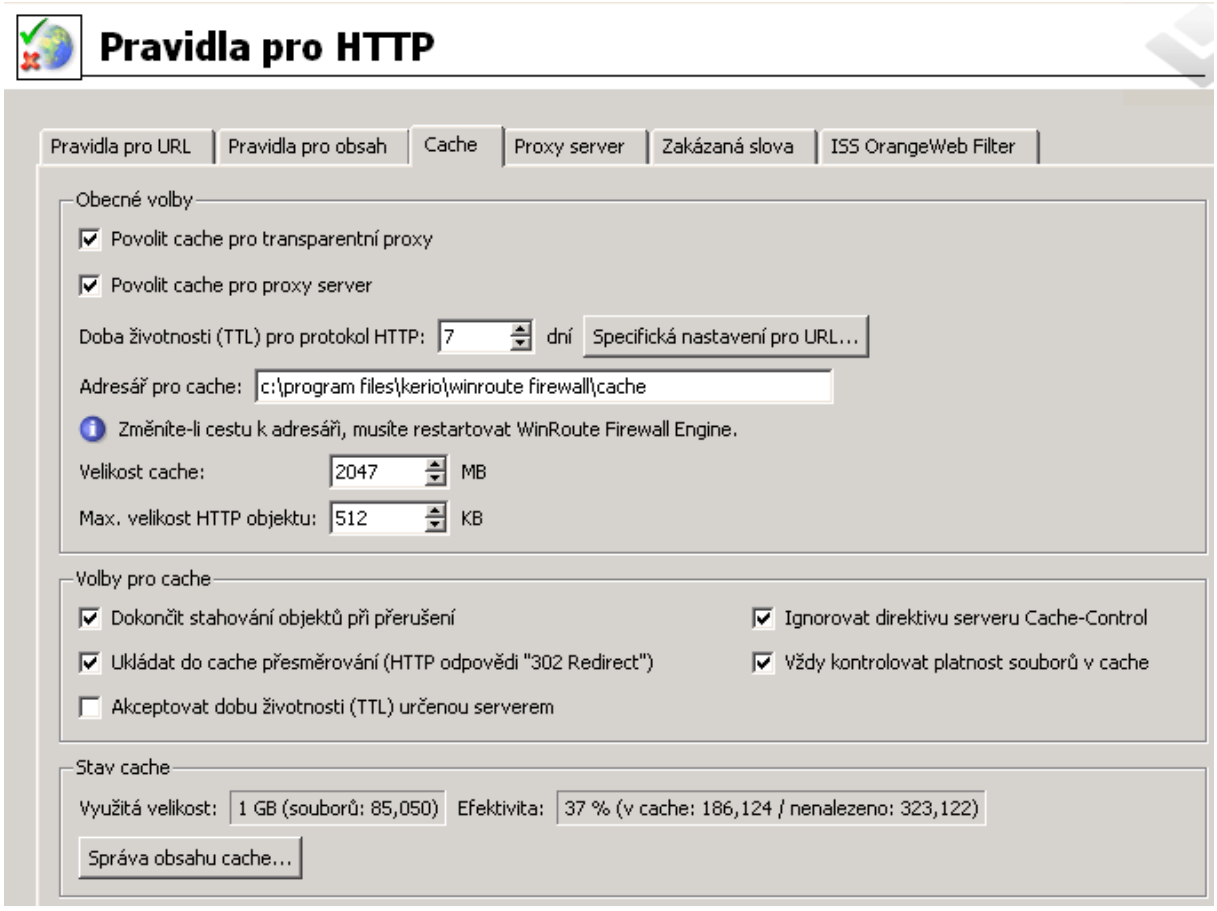
Povolit cache pro proxy server

Zapnutí cache pro HTTP komunikaci přes proxy server ve *WinRoute* (viz kapitola 8.4).

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*)



Obrázek 8.16 Nastavení parametrů HTTP cache

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 příštím startu *WinRoute Firewall Engine*. Staré soubory cache v původním adresáři budou automaticky odstraněny.

Velikost cache

Velikost souboru cache na disku. Maximální velikost cache je omezena na *2 GB* (*2047 MB*) *Poznámka:*

1. 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).
2. Uvedená maximální velikost cache platí pro *WinRoute* od verze *6.2.0*. Starší verze umožňovaly nastavení cache až do velikosti *4 GB* (tento limit byl snížen z technických důvodů). Je-li při startu *WinRoute Firewall Engine* detekována cache větší než *2047 MB*, pak je její velikost automaticky snížena na tuto hodnotu.

3. Při nastavení velikosti cache větší než je aktuální volné místo na příslušném disku se cache neinicializuje a do záznamu *Error* (viz kapitola 22.8) se zapíše odpovídající chybové hlášení.

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.
- *Ukládat do cache přesměrování (HTTP odpovědi 302 Redirect)* — tato volba obecně urychluje přístup na přesměrované WWW stránky.
  Odpovědi *302 Redirect* se za normálních okolností do cache neukládají. Návratový kód *302* protokolu *HTTP* znamená dočasné přesměrování — toto přesměrování může být kdykoliv zrušeno nebo se může měnit cílové URL. Při použití odpovědi z cache může být v některých případech klient přesměrován na již neaktuální nebo neplatné URL.
- *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.

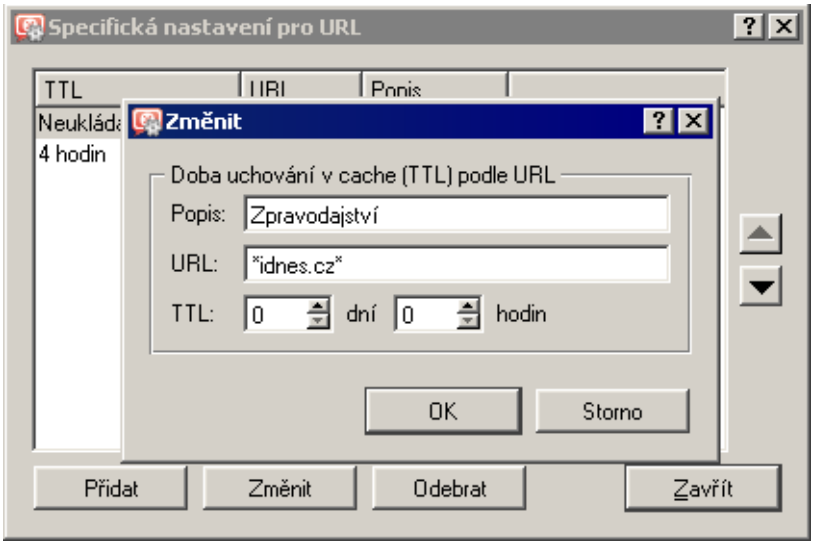
- *Ignorovat direktivu serveru Cache-Control* — po zapnutí této volby bude *WinRoute* ignorovat direktivy pro řízení cache na WWW stránkách.
  Pokud se obsah nějaké stránky velmi často mění, její autor na ni zpravidla umístí direktivu, aby se neukládala do cache. V některých případech je tato direktiva 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 kontrolovat 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). Např. v prohlížečích *Internet Explorer* a *Firefox/SeaMonkey* lze tuto kontrolu vyvolat 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.



Obrázek 8.17 HTTP cache — specifická nastavení pro 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/*`)

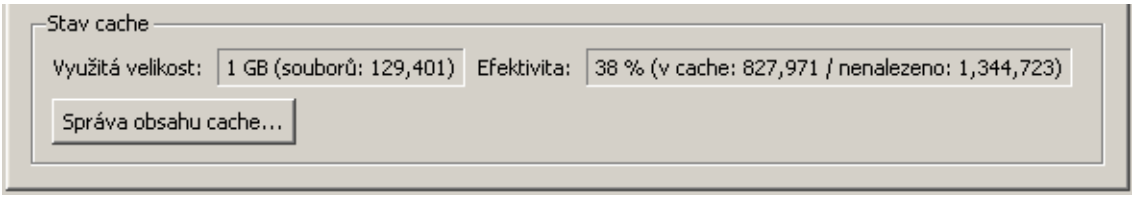
TTL

Doba platnosti objektů vyhovujících uvedenému URL.
Volba *0 dní, 0 hodin* znamená, že objekty nebudou do cache ukládány.

Sledování stavu a správa cache

WinRoute umožňuje sledovat využití HTTP cache a prohlížet, případně mazat objekty v cache uložené.

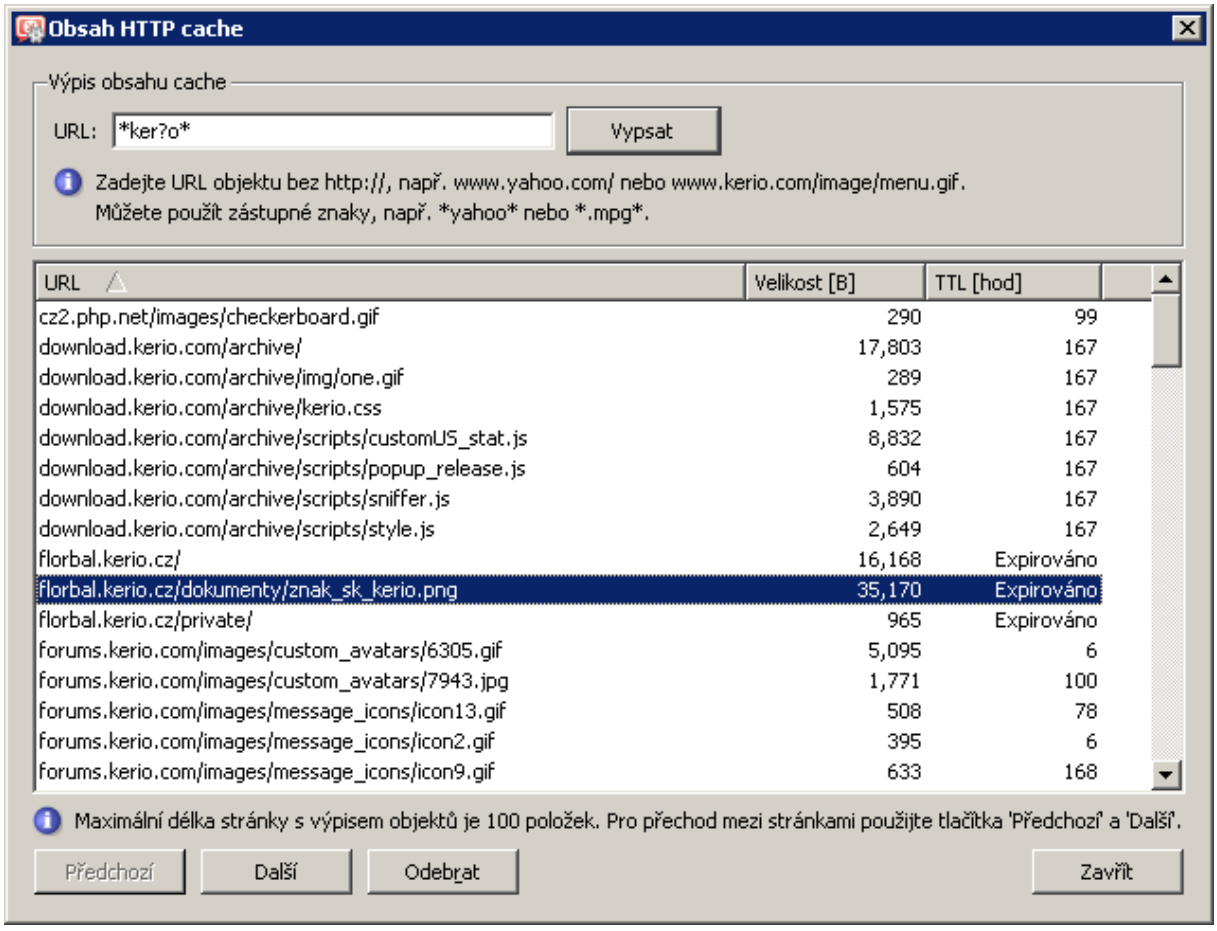
V dolní části záložky *Cache* se zobrazují základní stavové informace: aktuální využitá velikost a efektivita cache. Efektivita vyjadřuje poměr počtu objektů, které byly nalezeny v cache (a nemusely tedy být stahovány ze serveru) k celkovému počtu HTTP požadavků (měřeno od startu *WinRoute Firewall Engine*). Efektivita cache závisí především na chování uživatelů (zda pravidelně navštěvují určité WWW stránky, zda více uživatelů přistupuje na tytéž stránky atd.), částečně ji lze také ovlivnit výše popsanými konfiguračními parametry. Pokud cache vykazuje trvale nízkou efektivitu (méně než 5 %), doporučujeme přehodnotit konfiguraci cache.



Obrázek 8.18 Informace o stavu HTTP cache

Tlačítko *Správa obsahu cache...* otevírá okno pro prohlížení, vyhledávání a mazání objektů uložených v cache.

Pro zobrazení objektů v cache je nutné nejprve zadat do položky *URL* specifikaci hledaného objektu. Objekt může být specifikován buď absolutním URL (bez protokolu) — např. `www.kerio.com/image/menu.gif` nebo jako podřetězec URL s použitím zástupných znaků `*` (nahrazení libovolného počtu znaků) a `?` (nahrazení právě jednoho znaku).



Obrázek 8.19 Okno pro správu obsahu HTTP cache

Příklad

Při zadání výrazu `*ker?o*` budou zobrazeny všechny objekty, jejichž URL obsahuje řetězce `kerio`, `kerbo` apod.

Každý řádek výpisu objektů obsahuje URL objektu, jeho velikost v bytech (B) a *zbývající* dobu životnosti v hodinách. Z důvodu přehlednosti a rychlosti zobrazování je výpis objektů stránkován po 100 položkách. Tlačítky *Předchozí* a *Další* lze přecházet mezi jednotlivými stránkami výpisu.

Tlačítkem *Odebrat* se označený objekt vymaže z cache.

Tip

Kliknutím a tažením, případně kliknutím s přidržením klávesy *Ctrl* nebo *Shift* lze označit více objektů najednou.

Kapitola 9

Omezování šířky pásma

Velmi častým problémem sdíleného internetového připojení je situace, kdy jeden uživatel (případně několik uživatelů současně) stahuje nebo odesílá velký objem dat, čímž zcela vyčerpá kapacitu internetové linky (tzv. šířku pásma). Ostatní uživatelé pak zaznamenají výrazné zpomalení internetové komunikace, v krajním případě i výpadky některých služeb (pokud např. dojde k překročení maximální doby odezvy).

Typicky největší problém nastává v případě, kdy jsou v důsledku přetížení linky omezeny nebo blokovány síťové služby — např. poštovní server, WWW server nebo internetová telefonie (VoIP). Jeden uživatel může stahováním nebo odesíláním svých dat ohrozit funkčnost celé sítě.

Modul *Omezování šířky pásma* ve *WinRoute* nabízí řešení nejčastějších problémů s přetížením sdílené internetové linky. Tento modul dokáže rozpoznat spojení, kterými se přenáší velké objemy dat, a vyhradit pro ně určitou část kapacity linky. Zbývající kapacita zůstává volná pro ostatní komunikaci (kde se nepřenáší velké objemy dat, ale může zde být důležitá např. doba odezvy).

9.1 Jak funguje a jak lze využít omezování šířky pásma?

Modul *Omezování šířky pásma* má dvě základní funkce:

Omezení rychlosti přenosů velkých objemů dat

WinRoute sleduje všechna spojení navázaná mezi lokální sítí a Internetem. Pokud spojení vyhodnotí jako přenos objemných dat, omezí rychlost přenosu dat na nastavenou hodnotu, aby toto spojení neblokovalo ostatní komunikaci. Na lokální komunikaci se omezování šířky pásma neaplikuje.

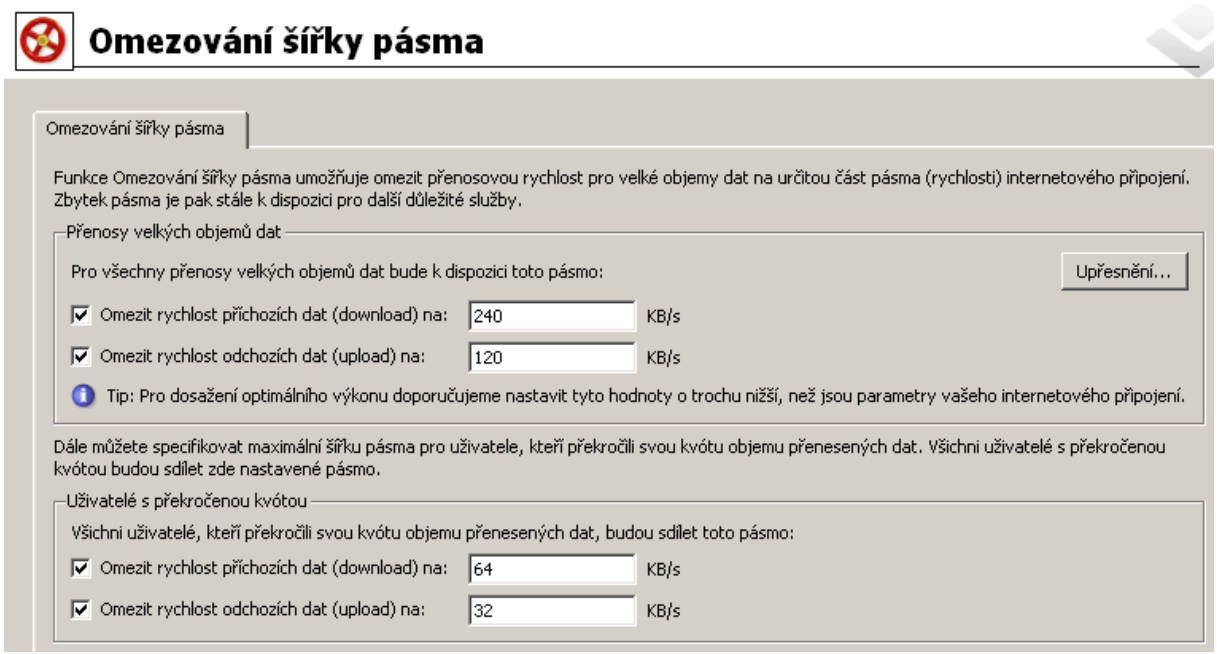
Poznámka: Omezování šířky pásma je nezávislé na komunikačních pravidlech.

Omezení rychlosti komunikace uživatelů s překročenou kvótou

O uživatelích, kteří překročili nastavenou kvótu objemu dat, lze předpokládat, že pravidelně stahují nebo odesílají velké množství dat. *WinRoute* umožňuje omezit těmto uživatelům rychlost přenosu dat, aby svou aktivitou neomezovali (resp. neblokovali) komunikaci ostatních uživatelů a síťových služeb. Na konkrétního uživatele je omezení aplikováno automaticky při překročení některého z nastavených limitů (viz kapitola 15.1).

9.2 Konfigurace omezování šířky pásma

Parametry modulu *Omezování šířky pásma* lze nastavit v sekci *Konfigurace* → *Omezování šířky pásma*.



Obrázek 9.1 Konfigurace modulu Omezování šířky pásma

Modul *Omezování šířky pásma* umožňuje nastavit omezení rychlosti příchozích dat (tj. z Internetu do lokální sítě) a odchozích dat (tj. z lokální sítě do Internetu) pro přenosy velkých objemů dat a pro uživatele, kteří překročili svou kvótu objemu přenesených dat. Jednotlivé limity jsou nezávislé, takže lze např. omezit pouze rychlost příchozích dat pro přenosy velkých souborů.

Upozornění

V modulu *Omezování šířky pásma* se všechny rychlosti se nastavují v kilobytech za sekundu (*KB/s*). Naproti tomu poskytovatelé internetového připojení zpravidla uvádějí kapacity linek v kilobitech za sekundu (*kbps*, *kbit/s* nebo *kb/s*), případně v megabitech za sekundu (*Mbps*, *Mbit/s* nebo *Mb/s*). Platí převodní vztah *1 KB/s = 8 kbit/s*.

Příklad: Linka *256 kbit/s* má rychlost *32 KB/s*, linka *1 Mbit/s* má rychlost *128 KB/s*.

Nastavení omezení

V horní části okna lze nastavit omezení pro přenosy velkých objemů dat. Hodnoty v těchto položkách určují, jaké pásmo bude vyhrazeno pro tyto přenosy. Zbývající pásmo bude stále k dispozici pro ostatní komunikaci.

Testováním bylo zjištěno, že optimálního využití kapacity internetové linky se dosáhne při nastavení hodnot blízkých parametrům připojení (cca 90%). Při nastavení vyšších hodnot je omezování šířky pásma neúčinné (při přenosech velkých objemů dat nezbude dostatek pásma pro ostatní služby), naopak při nastavení nižších hodnot nebude ve většině případů možné využít plnou kapacitu linky.

Upozornění

Pro nastavení optimálních hodnot je třeba uvažovat *skutečnou* kapacitu linky — zpravidla se nelze spoléhat na údaje, které uvádí poskytovatel internetového připojení. Jednou z možností, jak zjistit skutečnou kapacitu linky, je sledování grafu zatížení internetového rozhraní (viz kapitola 20.2) při velké zátěži, kdy je pravděpodobné, že je linka plně využita.

V dolní části okna lze nastavit omezení rychlosti příchozích a odchozích dat pro uživatele, kteří překročili svou kvótu objemu přenesených dat. Nastavené pásmo sdílí všichni uživatelé s překročenou kvótou. To znamená, že celková komunikace všech těchto uživatelů může zabrat nejvýše zde nastavenou šířku pásma.

Pro omezení uživatelů s překročenou kvótou objemu přenesených dat neexistují žádné optimální hodnoty. Záleží na uvážení správce *WinRoute*, jakou část pásma těmto uživatelům umožní využít. Doporučujeme nastavit takové hodnoty, aby uživatelé s překročenou kvótou svou aktivitou neomezovali ostatní uživatele a služby.

Poznámka: Konkrétnímu uživateli lze v případě překročení kvóty zcela zablokovat další komunikaci. Výše popsaná omezení budou aplikována pouze v případě, pokud je v příslušném uživatelském účtu nastaveno *Neblokovat komunikaci (pouze omezit rychlost...)*. Podrobnosti viz kapitola 15.1.

Upřesňující nastavení

Tlačítkem *Upřesnění* se otevírá dialog pro nastavení upřesňujících parametrů modulu *Omezování šířky pásma*. Tyto parametry se vztahují pouze na omezování přenosů velkých objemů dat, nemají vliv na omezování uživatelů s překročenou kvótou objemu přenesených dat (na tyto uživatele je omezení aplikováno vždy a na veškerou jejich komunikaci).

Specifikace služeb

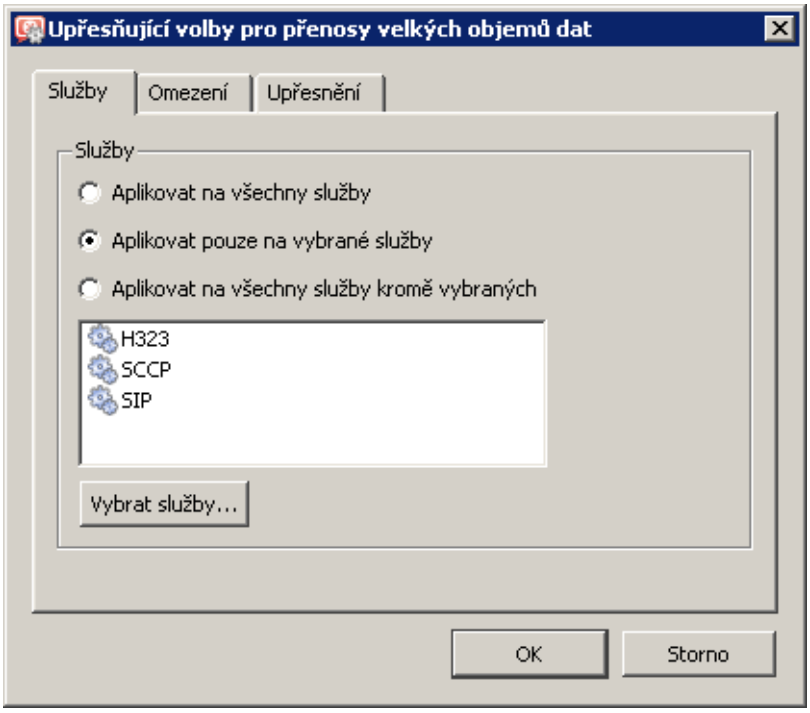
Některé služby mohou vykazovat charakteristiky přenosů objemných dat, přestože tomu tak ve skutečnosti není. Typickým příkladem je internetová telefonie (*Voice over IP — VoIP*). Pro takové služby je možné definovat výjimky, aby na ně nebylo aplikováno omezení šířky pásma.

Naopak může také vzniknout požadavek aplikovat omezení šířky pásma pouze na určité síťové služby (např. chceme omezit přenos souborů protokoly *FTP* a *HTTP*).

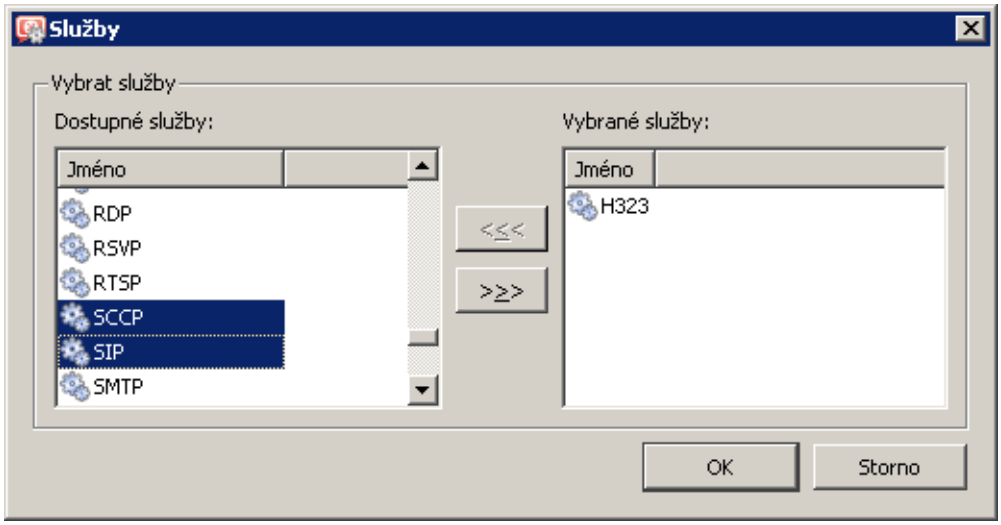
V záložce *Služby* můžeme definovat, na které služby má být omezení šířky pásma aplikováno:

- *Všechny služby* — omezení bude aplikováno na veškerou komunikaci mezi lokální sítí a Internetem.
- *Vybrané služby* — omezení bude aplikováno pouze na vybrané síťové služby. Komunikace ostatních služeb nebude omezována.
- *Všechny služby kromě vybraných* — komunikace vybraných služeb nebude omezována. Na všechny ostatní služby bude omezení aplikováno.

Tlačítko *Vybrat služby* otevírá dialog pro výběr síťových služeb. Přidržením klávesy *Ctrl* nebo *Shift* lze označit více služeb najednou. K dispozici jsou všechny síťové služby definované v sekci *Konfigurace* → *Definice* → *Služby* (viz kapitola 14.3).



Obrázek 9.2 Omezování šířky pásma — síťové služby



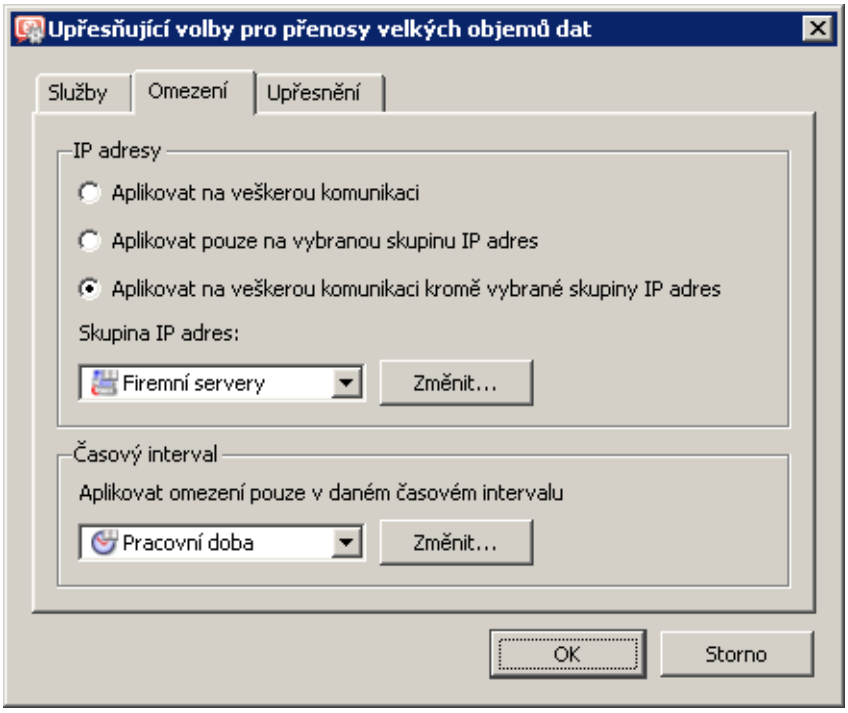
Obrázek 9.3 Omezování šířky pásma — výběr síťových služeb

IP adresy a časový interval

Častým požadavkem je aplikovat omezení šířky pásma pouze na některé počítače (např. nechceme omezovat poštovní server v lokální síti či komunikaci s firemním WWW serverem v Internetu). Skupina IP adres pro toto omezení může obsahovat libovolné IP adresy v lokální síti nebo v Internetu. Pokud mají pracovní stanice uživatelů pevné IP adresy, můžeme tímto způsobem aplikovat omezení i na jednotlivé uživatele.

Omezení šířky pásma může být rovněž aplikováno jen v určitém časovém intervalu (např. v pracovní době).

Tyto podmínky lze nastavit v záložce *Omezení*.



Obrázek 9.4 Omezování šířky pásma — skupina IP adres a časový interval

V horní části záložky *Omezení* lze vybrat způsob, jakým bude omezení dle IP adres aplikováno, a skupinu IP adres:

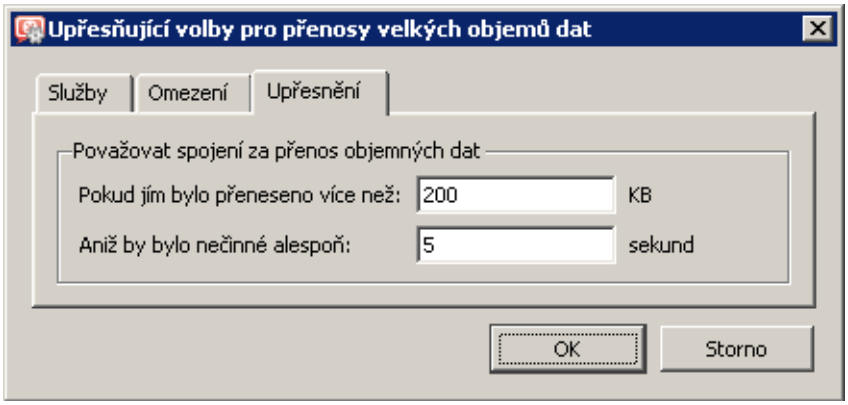
- *Na veškerou komunikaci* — skupina IP adres je irelevantní, pole pro výběr skupiny je neaktivní.
- *Pouze na vybranou skupinu IP adres* — omezení bude aplikováno pouze v případě, pokud IP adresa některého konce spojení patří do vybrané skupiny. Ostatní komunikace nebude omezena.
- *Na veškerou komunikaci kromě vybrané skupiny IP adres* — omezení nebude aplikováno v případě, pokud IP adresa některého konce spojení patří do vybrané skupiny. Ostatní komunikace bude omezena.

V dolní části záložky *Omezení* lze nastavit časový interval, ve kterém bude šířka pásma omezována. Tlačítko *Změnit* umožňuje upravit vybraný časový interval nebo vytvořit nový interval (podrobnosti viz kapitola 14.2).

Nastavení parametrů detekce přenosu velkého objemu dat

V záložce *Upřesnění* lze nastavit parametry detekce přenosu velkého objemu dat — minimální objem přenesených dat a mezní dobu nečinnosti (délku prodlevy). Výchozí hodnoty (*200 KB* a *5 sec*) jsou optimalizovány na základě dlouhodobého testování v reálném provozu.

Důrazně upozorňujeme, že experimenty s těmito hodnotami povedou ve většině případů k výraznému zhoršení funkčnosti modulu Omezování šířky pásma. S výjimkou speciálních případů (testování) striktně doporučujeme neměnit výchozí hodnoty!



Obrázek 9.5 Omezování šířky pásma — nastavení detekce přenosu velkého objemu dat

Podrobný popis principu detekce přenosů velkých objemů dat je uveden v kapitole 9.3.

9.3 Detekce spojení přenášejících velký objem dat

V této kapitole uvádíme popis způsobu, jakým modul *Omezování šířky pásma* detekuje spojení přenášející velké objemy dat. Tento popis slouží pouze jako doplňující informace — pro použití modulu *Omezování šířky pásma* není znalost principu detekce nutná.

Síťová komunikace každé služby má specifický průběh. Např. WWW prohlížeč typicky při přístupu na stránku otevře jedno nebo více spojení, přenese jimi určité množství dat (jednotlivé objekty na stránce) a tato spojení uzavře. Terminálové služby (např. *Telnet*, *SSH* apod.) mají obvykle otevřené spojení, kterým se přenáší malé množství dat s velkými prodlevami. Pro přenos velkých souborů je typický kontinuální tok dat s minimálními prodlevami.

U každého spojení se vyhodnocují dva parametry: objem přenesených dat a délka největší prodlevy. Pokud je spojením přenesen stanovený objem dat, aniž by nastala prodleva o stanovené minimální délce, je toto spojení považováno za přenos velkého objemu dat a budou na něj aplikována příslušná omezení.

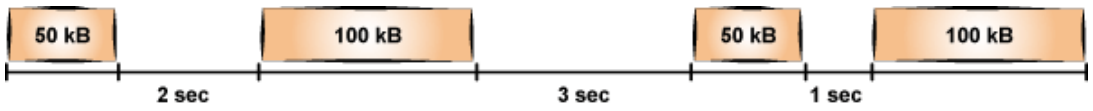
Je-li zaznamenána prodleva delší než stanovená hodnota, pak se vynuluje čítač objemu přenesených dat a počínaje dalším blokem dat probíhá další vyhodnocování výše popsaným způsobem. Z toho vyplývá, že za přenos velkého objemu dat je považováno každé takové spojení, které *kdykoliv* vykáže uvedené charakteristiky.

Mezní hodnota objemu přenesených dat a minimální prodleva jsou konfigurační parametry modulu *Omezování šířky pásma* (viz kapitola 9.2).

Příklady

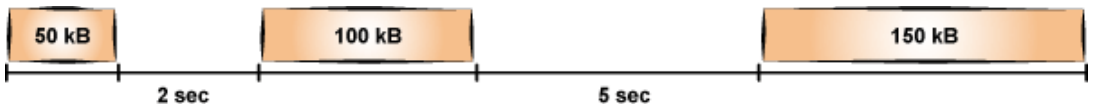
Pro snazší pochopení principu detekce spojení přenášejících velký objem dat uvádíme několik typických příkladů. Předpokládejme výchozí nastavení parametrů detekce: spojením musí být přeneseno alespoň *200 KB* dat, aniž by nastala prodleva alespoň *5 sec*.

1. Spojení na obrázku 9.6 je po přenesení třetího bloku dat považováno za přenos velkého souboru. V tomto okamžiku je spojením přeneseno 200 KB dat a nejdelší zaznamenaná prodleva je pouze 3 sec.



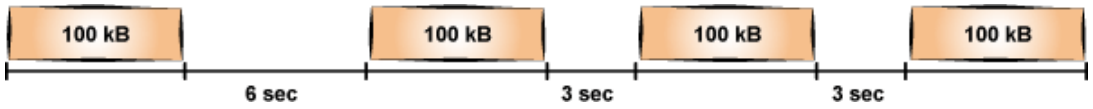
Obrázek 9.6 Příklad spojení — krátké prodlevy

2. Spojení na obrázku 9.7 není považováno za přenos velkého souboru, protože po přenesení 150 KB dat nastala prodleva 5 sec a pak již tímto spojením bylo přeneseno pouze 150 KB dat.



Obrázek 9.7 Příklad spojení — dlouhá prodleva

3. Spojením na obrázku 9.8 je přeneseno 100 KB dat, načež nastává prodleva 6 sec. Čítač objemu přenesených dat se tedy nuluje. Dále jsou přeneseny tři bloky dat o velikosti 100 KB. Po přenesení třetího bloku dat je zaznamenáno 200 KB přenesených dat (od poslední dlouhé prodlevy). Protože mezi druhým a třetím blokem je prodleva pouze 3 sec, je spojení po přenesení třetího bloku dat vyhodnoceno jako přenos velkého souboru.



Obrázek 9.8 Příklad spojení — dlouhá prodleva na začátku

Kapitola 10

Ověřování uživatelů

WinRoute umožňuje kontrolu přístupu (filtrování paketů/spojení, WWW stránek a FTP objektů a příkazů) také na základě uživatelů a/nebo skupin. Uživatelské jméno ve filtrovacím pravidle má význam IP adresy počítače, z něhož je tento uživatel přihlášen (resp. všech počítačů, z nichž je v daném okamžiku přihlášen). Analogicky skupina uživatelů má význam IP adres všech počítačů, ze kterých jsou právě přihlášeni členové této skupiny.

Kromě omezování přístupu lze přihlašování uživatelů využít také pro sledování jejich aktivit v rozhraní *Kerio StaR* (viz kapitola 21), v záznamech (viz kapitola 22), přehledu otevřených spojení (viz kapitola 19.2) a přehledu počítačů a uživatelů (viz kapitola 19.1). Není-li z určitého počítače přihlášen žádný uživatel, objeví se v záznamech a přehledech pouze IP adresa tohoto počítače. Ve statistikách bude komunikace tohoto počítače zahrnuta do skupiny *nepřihlášení uživatelé*.

10.1 Ověřování uživatelů na firewallu

Ověřit na firewallu se může každý uživatel, který má ve *WinRoute* vytvořen uživatelský účet (bez ohledu na přístupová práva). Uživatel se může k firewallu přihlásit těmito způsoby:

- Ručně — ve svém prohlížeči otevře WWW rozhraní *WinRoute*
  `https://server:4081/` nebo `http://server:4080/`
  (jméno serveru a čísla portů jsou pouze ilustrativní — viz kapitola 11).
  Alternativou je přihlášení k prohlížení webových statistik (viz kapitola 21) na adrese
  `https://server:4081/star` nebo `http://server:4080/star`
  Poznámka: Přihlášením do rozhraní *Web Administration* na adrese
  `https://server:4081/admin` nebo `http://server:4080/admin`
  k ověření uživatele na firewallu nedochází!
- Automaticky — každému uživateli mohou být přiřazeny IP adresy počítačů, ze kterých bude automaticky ověřován. V praxi to znamená, že při detekci komunikace z příslušného počítače *WinRoute* předpokládá, že na něm pracuje odpovídající uživatel, a považuje jej za přihlášeného z této IP adresy. Uživatel se samozřejmě může přihlásit i z jiných počítačů (některou z výše uvedených metod).
  IP adresy pro automatické ověřování lze nastavit v definici uživatelského účtu (viz kapitola 15.1).
  Tento způsob ověřování není vhodný pro případy, kdy na jednom počítači pracují střídavě různí uživatelé (mohlo by snadno dojít ke zneužití identity automaticky přihlášeného uživatele).
- Přesměrováním při přístupu na WWW stránky (pokud není na konkrétní stránku explicitně povolen přístup nepřihlášeným uživatelům — viz kapitola 12.2).

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: Uživatelé budou přesměrováváni na zabezpečené nebo nezabezpečené WWW rozhraní, podle toho, která verze WWW rozhraní je povolena (viz kapitola 11.1). Jsou-li povoleny obě verze, bude použito zabezpečené WWW rozhraní.

- Prostřednictvím NTLM — je-li použit prohlížeč *Internet Explorer* nebo *Firefox/SeaMonkey* a uživatel se ověřuje v doméně *Windows NT* nebo *Active Directory*, pak může být ověřen zcela automaticky (přihlašovací stránka se vůbec nezobrazí). Podrobnosti viz kapitola 25.3.

Upřesňující parametry pro ověřování uživatelů

V sekci *Uživatelé a skupiny* → *Uživatelé*, záložka *Volby pro ověřování*, lze nastavit parametry pro přihlašování a odhlašování uživatelů na/z firewall.

Obrázek 10.1 Volby pro ověřování uživatelů na firewallu

Přesměrování na přihlašovací stránku

Po zapnutí volby *Při přístupu na WWW stránky vždy vyžadovat ověření uživatele* bude vyžadováno ověření uživatele při přístupu na libovolnou WWW stránku (pokud není dosud přihlášen). Vyžádání ověření se liší podle způsobu, jakým WWW prohlížeč přistupuje do Internetu:

- *Přímý přístup* — prohlížeč bude automaticky přesměrován na přihlašovací stránku WWW rozhraní *WinRoute* (viz kapitola 11.2) a po úspěšném přihlášení na požadovanou WWW stránku.
- *Přístup přes proxy server ve WinRoute* — prohlížeč nejprve zobrazí přihlašovací dialog, a teprve po úspěšném přihlášení požadovanou WWW stránku.

Bude-li volba *Při přístupu na WWW stránky vždy vyžadovat ověření uživatele* vypnuta, pak bude ověření uživatele vyžadováno pouze při přístupu na WWW stránky, na které není pravidly pro URL povolen přístup nepřihlášeným uživatelům (viz kapitola 12.2).

Poznámka: Ověření uživatele má význam nejen pro řízení přístupu na WWW stránky (případně k dalším službám), ale také pro sledování aktivit jednotlivých uživatelů — využívání Internetu není anonymní.

Vyžadovat ověření na netransparentním proxy serveru

Za normálních okolností, pokud se uživatel k firewallu přihlásí z určitého počítače, pak je považován za ověřeného z IP adresy tohoto počítače až do okamžiku, kdy se odhlásí nebo kdy je automaticky odhlášen při nečinnosti (viz níže). Pokud však klientský počítač umožňuje práci více uživatelů současně (např. *Microsoft Terminal Services*, *Citrix Presentation Server* nebo *Rychlé přepínání uživatelů* v systémech *Windows XP*, *Windows Server 2003*, *Windows Vista* a *Windows Server 2008*), pak bude firewall vyžadovat ověření pouze po uživateli, který začal pracovat jako první. Ostatní uživatelé pak budou vystupovat pod jeho identitou.

Pro služby *HTTP* a *HTTPS* lze toto technické omezení obejít. Ve WWW prohlížečích všech klientů víceuživatelského systému nastavíme přístup do Internetu přes proxy server ve *WinRoute* (podrobnosti viz kapitola 8.4) a ve *WinRoute* zapneme volbu *Povolit ověřování na netransparentním proxy serveru*. Proxy server pak bude vyžadovat ověření uživatele při zahájení každé nové relace prohlížeče[5].

Vyžadování ověření uživatele na proxy serveru při zahájení každé nové relace může být však obtěžující pro uživatele pracující na „jednouživatelských “ počítačích. Proto je vhodné omezit vyžadování ověření v každé relaci pouze na počítače, o kterých víme, že na nich pracuje více uživatelů. K tomuto účelu slouží volba *Aplikovat pouze na tyto IP adresy*.

Automatické ověřování (NTLM)

Je-li zapnuta volba *Povolit WWW prohlížečům...*, pak při použití prohlížeče *Internet Explorer* (verze 5.01 a vyšší) nebo *Firefox/SeaMonkey* (verze jádra 1.3 a vyšší), pak může být uživatel ověřován na firewallu automaticky (metodou NTLM).

V praxi to znamená, že prohlížeč nepožaduje zadání uživatelského jména a hesla a použije identitu uživatele přihlášeného do systému *Windows*. V jiných operačních systémech metoda NTLM bohužel není k dispozici.

Podrobnosti naleznete v kapitole 25.3.

[5] *Relace* (angl. *session*, někdy též překládáno jako *sezení*) je období běhu jedné instance prohlížeče. Např. v případě prohlížečů *Internet Explorer*, *Firefox* nebo *Opera* relace zaniká po uzavření všech otevřených oken prohlížeče, zatímco u prohlížeče *SeaMonkey* relace zaniká až po ukončení programu *Rychlé spuštění* (ikona v oznamovací oblasti nástrojové lišty).

Automatické odhlášení uživatele při nečinnosti

V položce *Časový limit* lze nastavit dobu (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).

Popsaná situace nastává zpravidla v případech, kdy se uživatel zapomene od firewallu odhlásit, a proto nedoporučujeme tuto volbu vypínat — 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).

Kapitola 11

WWW rozhraní

WinRoute obsahuje speciální WWW server, který poskytuje rozhraní pro prohlížení statistik (*Kerio StaR*), pro nastavení některých parametrů uživatelského účtu a pro správu firewallu prostřednictvím WWW prohlížeče (*Web Administration*). WWW rozhraní existuje ve dvou verzích: nezabezpečené a zabezpečené SSL (obě verze obsahují totožné stránky).

Nezabezpečenou verzi WWW rozhraní otevřeme zadáním následujícího URL (`server` má význam jména nebo IP adresy počítače s *WinRoute* a 4080 je standardní port WWW rozhraní):

```
http://server:4080/
```

Pro zabezpečenou verzi je třeba uvést protokol HTTPS a port zabezpečeného WWW rozhraní (standardně 4081):

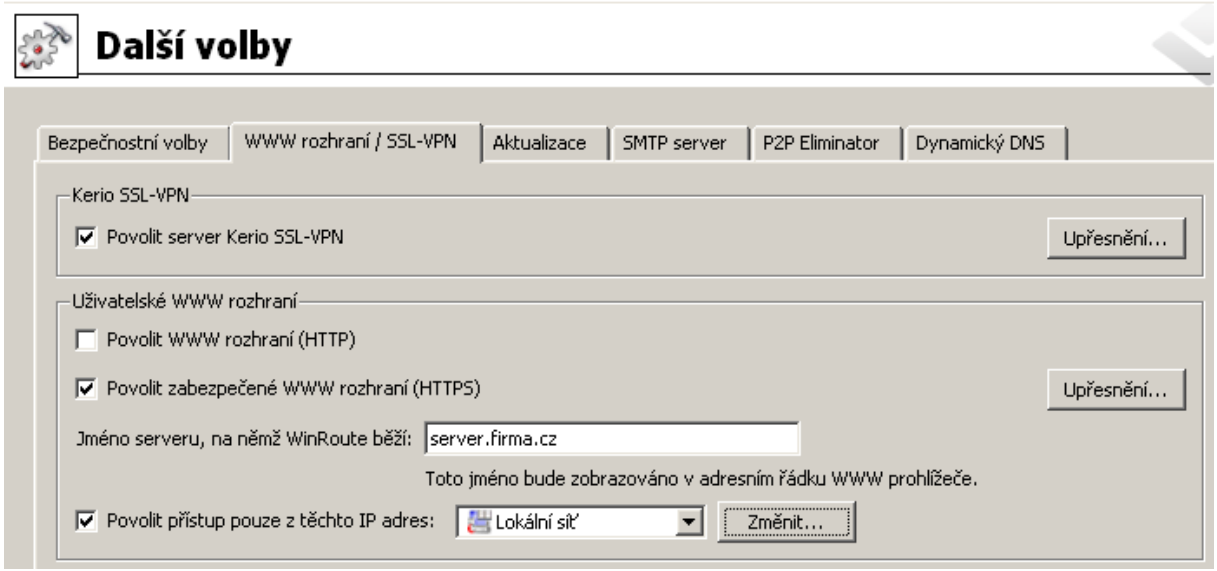
```
https://server:4081/
```

Tato kapitola se zabývá nastavením parametrů WWW rozhraní v administračním programu *WinRoute*. *Kerio StaR* a uživatelské WWW rozhraní jsou podrobně popsány v manuálu *Kerio WinRoute Firewall — Příručka uživatele*.

11.1 Volby pro WWW rozhraní

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

Poznámka: Ve *WinRoute* pro systém *Windows* obsahuje záložka *WWW rozhraní* také volby pro rozhraní *Kerio SSL-VPN*. Tato komponenta je podrobně popsána v kapitole 24.



Obrázek 11.1 Nastavení parametrů WWW rozhraní WinRoute

Povolit WWW rozhraní (HTTP)

Tato volba zapíná nezabezpečenou (HTTP) verzi WWW rozhraní. Výchozí port nezabezpečeného WWW rozhraní je 4080.

Poznámka: Nevýhodou nezabezpečeného WWW rozhraní je možnost odposlechu síťové komunikace a následného zneužití přihlašovacích informací uživatelů. Z tohoto důvodu by mělo být preferováno použití zabezpečeného WWW rozhraní.

Povolit zabezpečené WWW rozhraní (HTTPS)

Tato volba zapíná zabezpečenou (HTTPS) verzi WWW rozhraní. Výchozí port zabezpečeného WWW rozhraní je 4081.

Jméno serveru, na němž *WinRoute* běží

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. Rovněž SSL certifikát pro zabezpečené WWW rozhraní (viz dále) by měl být vystaven na toto jméno serveru.

Zadané jméno serveru se rovněž používá, pokud *WinRoute* potřebuje přesměrovat prohlížeč uživatele na přihlašovací stránku (např. pokud neověřený uživatel přistupuje na WWW stránku, pro kterou je vyžadováno ověření — viz kapitoly 10.1 a 12.2).

Poznámky:

1. Pokud všichni klienti, kteří na WWW rozhraní přistupují, používají jako DNS server modul *DNS* ve *WinRoute*, pak není nutné jméno serveru do DNS přidávat — modul *DNS* jej přečte automaticky z této položky (a provede rovněž kombinaci se jménem lokální domény — viz kapitola 8.1).
2. V edici *Software Appliance / VMware Virtual Appliance* se do této položky automaticky dosazuje jméno serveru nastavené v záložce *Systémová konfigurace* — viz kapitola 16.1.

Povolit přístup pouze z těchto IP adres

Výběr skupiny IP adres, z níž bude k WWW rozhraní povolen přístup (typicky lokální síť). Tlačítkem *Změnit* lze upravit vybranou skupinu IP adres nebo vytvořit novou (podrobnosti viz kapitola 14.1).

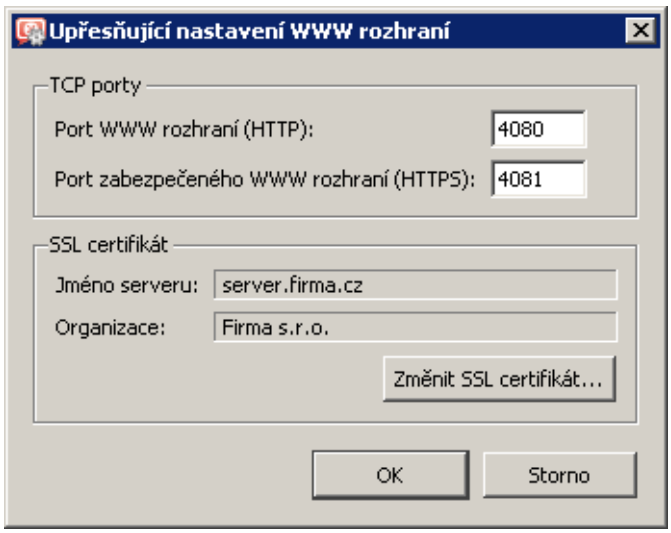
Omezení přístupu se vztahuje k nezabezpečené i zabezpečené verzi WWW rozhraní.

Tlačítko *Upřesnění* otevírá dialog pro nastavení dalších parametrů WWW rozhraní.

Nastavení portů WWW rozhraní

Sekce *TCP porty* umožňuje nastavit čísla portů nezabezpečeného a zabezpečeného WWW rozhraní (výchozí porty jsou 4080 pro nezabezpečené rozhraní a 4081 pro zabezpečené rozhraní).

Tip: Pokud na počítači s *WinRoute* není provozován žádný WWW server, pak lze pro nezabezpečené WWW rozhraní *WinRoute* použít standardní port protokolu HTTP (tj. port 80) a pro zabezpečené WWW rozhraní standardní port protokolu HTTPS (tj. port 443). Při použití standardních portů pak není nutné uvádět číslo portu v adresách stránek WWW rozhraní.



Obrázek 11.2 Nastavení portů WWW rozhraní WinRoute

Ve *WinRoute* pro systém *Windows* však standardní port protokolu HTTPS (443) využívá rozhraní *Clientless SSL-VPN* (viz kapitola 24), a proto jej ve výchozí konfiguraci nelze použít pro zabezpečené WWW rozhraní.

Upozornění

Zadáte-li do některé z uvedených položek port, který již používá jiná služba nebo aplikace, pak po stisknutí tlačítka *Použít* (v sekci *Konfigurace* → *Další volby*) *WinRoute* tento port sice akceptuje, ale WWW rozhraní se na něm nespustí a do záznamu *Error* (viz kapitola 22.8) se vypíše chybové hlášení v této podobě:

```
Socket error: Unable to bind socket for service to port 80.
(5002) Failed to start service "WebInterface"
bound to address 192.168.1.10.
```

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.

SSL certifikát pro WWW rozhraní

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

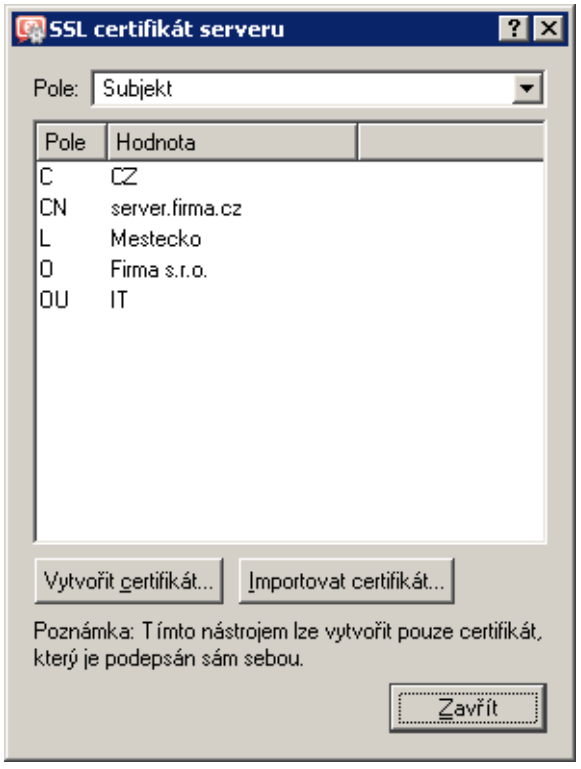
byla zaručena pravost certifikátu, musí být ověřen a podepsán třetí stranou, tzv. certifikační autoritou.

Komunikace mezi klientem a serverem pak vypadá následovně: Klient vygeneruje klíč pro symetrickou šifru 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. Tento klíč se pak použije pro šifrování a dešifrování veškeré další komunikace.

Import nebo vytvoření SSL certifikátu

Při instalaci *WinRoute* je automaticky vytvořen testovací certifikát pro zabezpečené WWW rozhraní (certifikát je uložen v podadresáři `sslcert` instalačního adresáře *WinRoute* v souboru `server.crt`, odpovídající privátní klíč v souboru `server.key`). Vytvořený certifikát je unikátní, je však vystaven na fiktivní jméno serveru a není vydán důvěryhodnou certifikační autoritou. Tento certifikát slouží pouze k zajištění funkce zabezpečeného WWW rozhraní (typicky pro zkušební účely) do chvíle, než vytvoříte nový certifikát nebo importujete certifikát vystavený veřejnou certifikační autoritou.

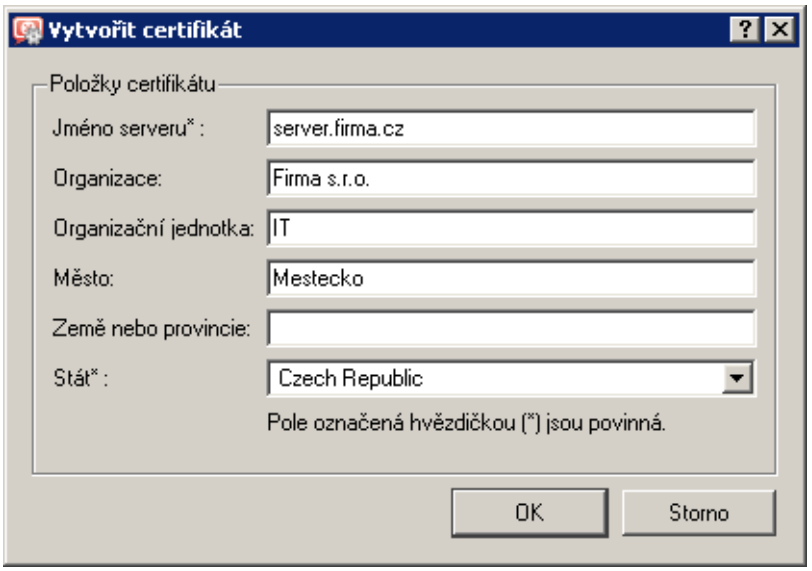
Po stisknutí tlačítka *Změnit SSL certifikát* (v dialogu pro nastavení upřesňujících parametrů WWW rozhraní) se zobrazí dialog s aktuálním certifikátem serveru. Volbou *Pole* (položka certifikátu) lze zobrazit údaje buď o vydavateli certifikátu nebo o subjektu — tedy vašem serveru.



Obrázek 11.3 SSL certifikát WWW rozhraní WinRoute

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

Můžete si vytvořit vlastní, tzv. self-signed certifikát („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 (*).



Obrázek 11.4 Vytvoření nového „self-signed“ certifikátu pro WWW rozhraní WinRoute

Po stisknutí tlačítka *OK* se nově vytvořený certifikát zobrazí v dialogu *SSL certifikát serveru* a ihned se začne používat (není třeba nic restartovat). Vytvořený certifikát bude uložen do souboru `server.crt` a odpovídající privátní klíč do souboru `server.key`.

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 certifikát již zajišťuje vašim klientům bezpečnost, protože je unikátní a 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 zakoupit plnohodnotný certifikát od některé veřejné certifikační autority (např. *Verisign*, *Thawte*, *SecureSign*, *SecureNet*, *Microsoft Authenticode* apod.).

Při importu certifikátu je třeba načíst soubor s certifikátem (`*.crt`) a odpovídající privátní klíč (`*.key`). Tyto soubory *WinRoute* uloží do podadresáře `sslcert` ve svém instalačním adresáři.

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

11.2 Přihlašování uživatelů k WWW rozhraní

Při přístupu k WWW rozhraní *WinRoute* je vyžadováno ověření uživatele. Do WWW rozhraní se může přihlásit každý uživatel, který má ve *WinRoute* vytvořen uživatelský účet. V závislosti na právu prohlížet statistiky (viz kapitola 15.2) se po přihlášení uživateli zobrazí rozhraní *Kerio StaR* nebo stránka se stavovými informacemi a osobními předvolbami.

Při použití účtů z více než jedné *Active Directory* domény (viz kapitola 15.4) platí pro uživatelské jméno tato pravidla:

- *Lokální uživatelský účet* — jméno musí být zadáno bez domény (např. `admin`),
- *Primární doména* — jméno může být zadáno bez domény (např. `jnovak`) nebo s doménou (např. `jnovak@firma.cz`),
- *Ostatní domény* — jméno musí být zadáno včetně domény (např. `pmaly@pobocka.firma.cz`).

Není-li mapována žádná nebo je-li mapována pouze jedna *Active Directory* doména, mohou se všichni uživatelé přihlašovat uživatelským jménem bez domény.

Poznámka: Přihlášení do WWW rozhraní je základní způsob ověření uživatele na firewallu. Další způsoby ověřování uživatel na firewallu jsou popsány v kapitole 10.1.

Kapitola 12

Filtrování protokolů HTTP a FTP

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 modulem *Kerio Web 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

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

12.1 Podmínky pro filtrování HTTP a FTP

Pro činnost filtrování obsahu protokolů HTTP a FTP musí být splněny tyto základní podmínky:

1. Komunikace musí být obsluhována příslušným inspekčním modulem.

Potřebný inspekční modul je aktivován automaticky, pokud není komunikačními pravidly explicitně určeno, že nemá být pro danou komunikaci použit. Podrobnosti najdete v kapitole 7.3.

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 7.3).

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

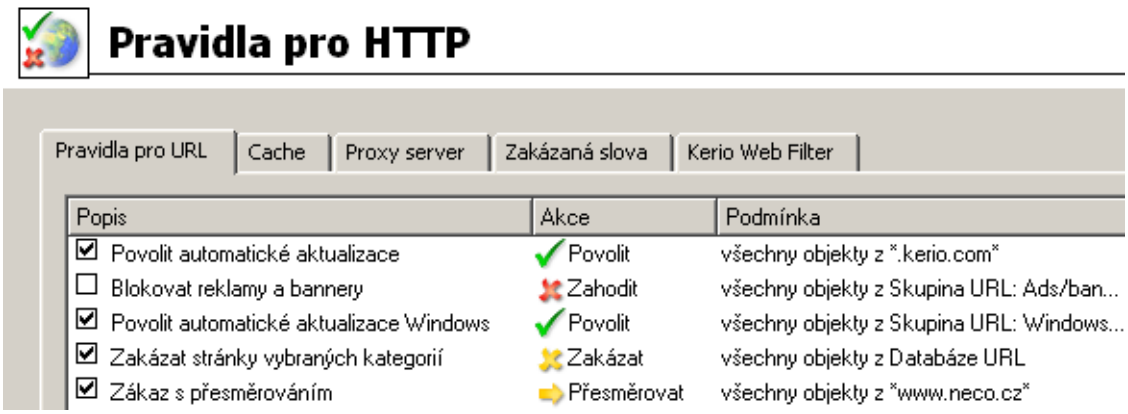
4. Pravidla pro HTTP i FTP se aplikují také při použití proxy serveru ve *WinRoute* (pak je podmínka 1. irelevantní). Protokol FTP však nelze filtrovat, pokud je použit nadřazený proxy server (podrobnosti viz kapitola 8.4). V takovém případě jsou pravidla pro FTP neaktivní.

5. Při použití proxy serveru (viz kapitola 8.4) je možné filtrovat také HTTPS servery (příklad: `https://secure.kerio.cz/`). Jednotlivé objekty na těchto serverech však již filtrovat nelze.

12.2 Pravidla pro URL

Pravidla pro URL umožňují řídit přístup uživatelů k WWW stránkám, jejichž URL vyhovují určitým kritériím. Doplňkovými funkcemi je filtrování stránek dle výskytu zakázaných slov, specifické blokování prvků WWW stránek (skripty, aktivní objekty atd.) a možnost vypnutí antivirové kontroly pro určité stránky.

K definici pravidel pro URL slouží stejnojmenná záložka v sekci *Konfigurace* → *Filtrování obsahu* → *Pravidla pro HTTP*.



Obrázek 12.1 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).

Poznámka: Přístup k URL, pro které neexistuje odpovídající pravidlo, je povolen všem přihlášeným uživatelům (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.

V záložce *Pravidla pro URL* mohou být zobrazeny tyto sloupce:

- *Popis* — textový popis pravidla (pro zvýšení přehlednosti). Zaškrtávací pole vlevo od popisu pravidla umožňuje pravidlo „zapnout“ a „vypnout“ (např. v případě, kdy má být pravidlo dočasně vyřazeno).
- *Akce* — akce, která bude provedena při splnění podmínek tohoto pravidla (*Povolit* — povolit přístup na stránku, *Zakázat* — zakázat přístup na stránku a zobrazit informaci o zákazu, *Zahodit* — zakázat přístup na stránku a zobrazit prázdnou stránku, *Přesměrovat* — přesměrovat na stránku uvedenou v pravidle).
- *Podmínka* — podmínka, za které pravidlo platí (URL vyhovuje určitým kritériím, stránka je klasifikována modulem *Kerio Web Filter* do určité kategorie atd.).
- *Vlastnosti* — upřesňující volby v pravidle (např. antivirová kontrola, filtrování zakázaných slov atd.).

Následující sloupce jsou ve výchozím nastavení skryty. Zobrazit je lze pomocí funkce *Nastavit sloupce* v kontextovém menu — podrobnosti viz kapitola 3.2.

- *Skupina IP adres* — skupina IP adres, pro kterou pravidlo platí. Jedná se o IP adresy klientů (tj. pracovních stanic uživatelů, kteří přes *WinRoute* přistupují k WWW stránkám).
- *Časová platnost* — časový interval, ve kterém pravidlo platí.
- *Seznam uživatelů* — výčet uživatelů a skupin uživatelů, na které se pravidlo vztahuje.

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.

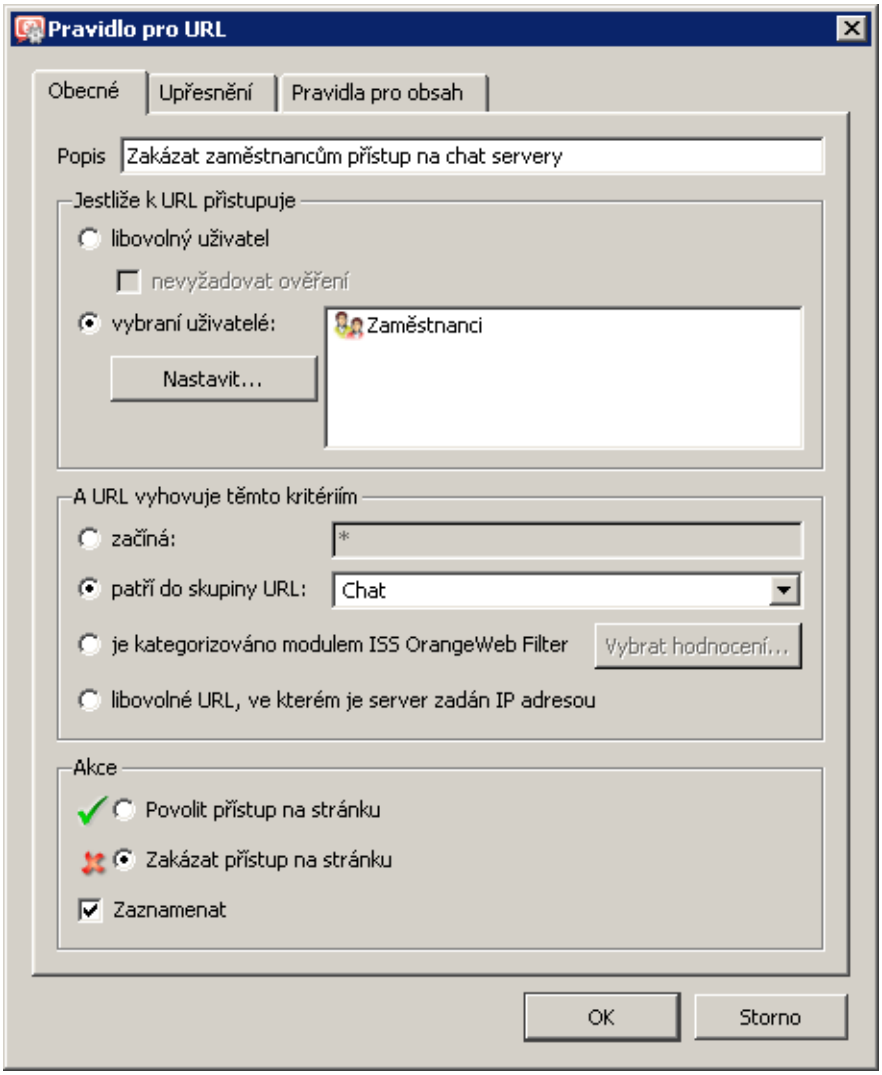
Definice pravidel pro URL

Chceme-li přidat nové pravidlo, označíme v tabulce pravidlo, pod které má být nové pravidlo vloženo, a stiskneme tlačítko *Přidat*. Šipkovými tlačítky na pravé straně okna lze pořadí pravidel dodatečně upravit.

Dialog pro definici nového pravidla:

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

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



Obrázek 12.2 Pravidlo pro URL — základní parametry

Jestliže k tomuto URL přistupuje

Volba, pro které uživatele bude toto pravidlo platit:

- *libovolný uživatel* — pro všechny uživatele přihlášené k firewallu.
  Zapnutím volby *nevyžadovat ověření* bude pravidlo platit také pro uživatele, kteří nejsou k firewallu přihlášeni (anonymní uživatele).
  Poznámka:

  1. Velmi častým požadavkem je, aby firewall vyžadoval ověření uživatelů při přístupu na libovolnou WWW stránku. Toho lze docílit globálním nastavením v sekci *Uživatelé*, záložka *Volby pro ověřování* (viz kapitola 15.1). S použitím volby *nevyžadovat ověření* můžeme pak např. definovat pravidlo povolující přístup na určité stránky bez přihlášení.
  2. Není-li ověření uživatelů vyžadováno, pak nemá volba *nevyžadovat ověření*

v pravidlech pro URL žádný účinek.

- *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: Jméno uživatele má v pravidle význam IP adresy počítače, ze kterého je uživatel v daném okamžiku přihlášen k firewallu (podrobnosti viz kapitola 10.1).

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 14.4), které má URL vyhovovat
- *je kategorizováno modulem Kerio Web Filter* — pravidlo bude platit pro všechny stránky, které modul *Kerio Web Filter* zařadí do některé z vybraných kategorií.
  Tlačítko *Vybrat hodnocení...* otevírá dialog pro výběr kategorií modulu *Kerio Web Filter*. Podrobnější informace naleznete v kapitole 12.3.
- *libovolné URL, ve kterém 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:

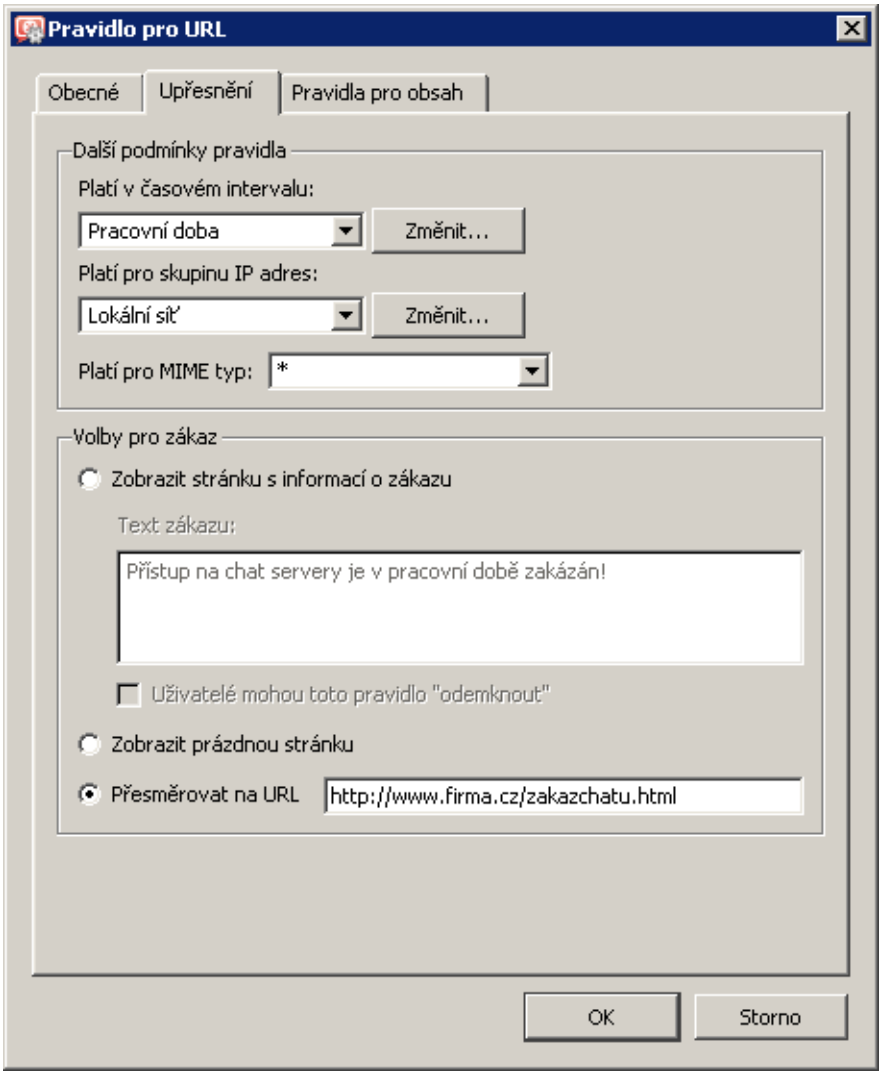
- *Povolit přístup na stránku*
- *Zakázat přístup na stránku* — požadovaná stránka bude blokována. Uživateli se zobrazí buď stránka s informací o zákazu, prázdná stránka nebo bude přesměrován na jinou stránku (dle nastavení v záložce *Upřesnění* — viz dále).

Zaškrtnutím volby *Zaznamenat* budou všechny přístupy na stránky, které vyhověly tomuto pravidlu, zaznamenávány do záznamu *Filter* (viz kapitola 22.9).

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 14.2).



Obrázek 12.3 Pravidlo pro URL — upřesňující parametry

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 14.1).

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 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 pravidla 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 *Security* (viz kapitola 22.11).
  Odemykat pravidla mohou pouze uživatelé, kteří mají příslušné právo (viz kapitola 15.1). Z toho vyplývá, že pravidla nikdy nemohou odemykat nepřihlášení (anonymní) uživatelé.
  Poznámka:
  1. Při jakékoliv změně v pravidlech pro URL se ihned ruší všechna odemknutí.
  2. Text zákazu nesmí z bezpečnostních a technických důvodů obsahovat žádné HTML tagy. Pokud prostý text nevyhovuje, doporučujeme použít přesměrování na jinou stránku (viz níže).
- Prázdnou stránku — uživatel nezíská žádné informace o tom, proč se požadovaná stránka nezobrazila (nedozví se ani o existenci *WinRoute*).
- Jinou stránku — prohlížeč uživatele bude přesměrován na zadané URL. Tuto volbu lze využít např. pro definici vlastní stránky s informací o zakázaném přístupu.

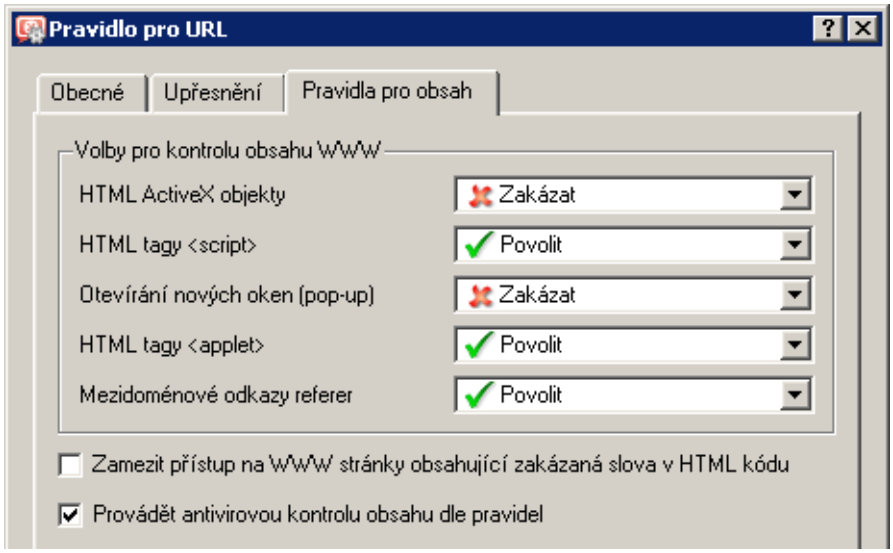
Záložka *Pravidla pro obsah* umožňuje nastavit pravidla pro filtrování určitých prvků WWW stránek. Parametry v této záložce lze nastavovat pouze v případě, že se jedná o pravidlo povolující přístup (v záložce *Obecné* je vybrána volba *Povolit přístup na stránku*).

Volby pro kontrolu obsahu WWW

V této sekci lze provést specifické nastavení filtrování objektů na WWW stránkách, které vyhovují tomuto pravidlu (podrobnosti viz kapitola 15.2). Specifické nastavení v pravidle pro URL má vyšší prioritu než nastavení v uživatelském účtu.

Zamezit přístup na WWW stránky...

Zapnutím této volby bude blokován přístup na WWW stránky, které vyhovují tomuto pravidlu a obsahují zakázaná slova definovaná v sekci *Konfigurace → Filtrování obsahu → Pravidla pro HTTP*, záložka *Zakázaná slova*.
Podrobné informace o zakázaných slovech viz kapitola 12.4.



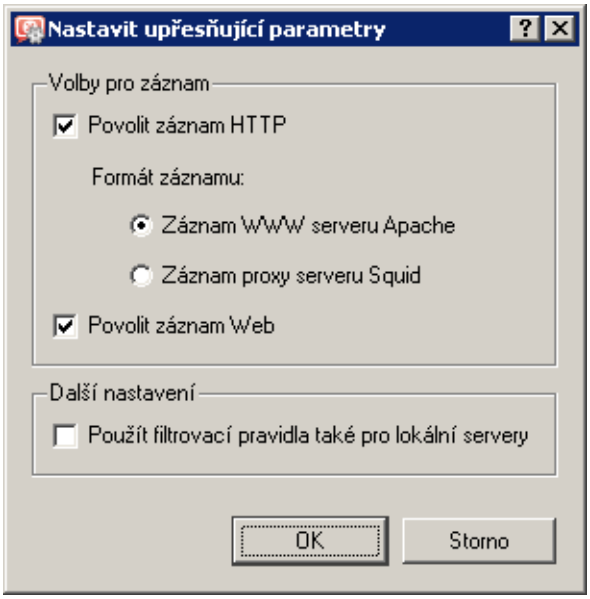
Obrázek 12.4 Volby pro obsah WWW stránek vyhovujících pravidlu pro URL

Provádět antivirovou kontrolu obsahu dle pravidel

Po zaškrtnutí této volby bude prováděna antivirová kontrola dle nastavení v sekci *Konfigurace* → *Filtrování obsahu* → *Antivirus* (viz kapitola 13.3).

Upřesňující parametry pro inspekci protokolu HTTP

Tlačítkem *Upřesnění* v záložce *Pravidla pro HTTP* se otevírá dialog pro nastavení parametrů inspekčního modulu protokolu HTTP.



Obrázek 12.5 Nastavení parametrů inspekčního modulu protokolu HTTP

Volby *Povolit záznam HTTP* a *Povolit záznam Web* zapínají/vypínají zápis HTTP požadavků (resp. navštívených WWW stránek) do záznamů *HTTP* (viz kapitola 22.10) a *Web* (viz kapitola 22.14).

U položky *Povolit záznam HTTP* může být vybrán i formát záznamu: záznam WWW serveru *Apache* (http://www.apache.org/) nebo záznam proxy serveru *Squid* (http://www.squid-cache.org/). Nastavení typu záznamu je důležité zejména v případě, má-li být záznam zpracováván nějakým analytickým nástrojem.

Ve výchozím nastavení jsou povoleny oba záznamy (*HTTP* i *Web*) a pro záznam *HTTP* je nastaven typ *Apache*, který je pro správce firewallu (člověka) čitelnější.

Volba *Použít filtrovací pravidla také pro lokální servery* určuje, zda budou pravidla pro filtrování obsahu aplikována také na WWW servery v lokální síti, které jsou komunikačními pravidly (viz kapitola 7) zpřístupněny z Internetu. Ve výchozím nastavení je tato volba vypnuta — inspekční modul kontroluje pouze syntaxi protokolu HTTP a provádí záznam požadavků (resp. WWW stránek) dle výše popsaných nastavení.

12.3 Hodnocení obsahu WWW stránek (Kerio Web Filter)

Modul *Kerio Web Filter*, integrovaný 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.

Kerio Web Filter používá celosvětovou dynamickou databázi, která obsahuje URL stránek a jejich klasifikace. Tuto databázi udržují speciální servery, které provádějí hodnocení jednotlivých stránek. Přistupuje-li uživatel k určité stránce, modul *Kerio Web 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: Používání modulu *Kerio Web Filter* je vázáno na speciální licenci (předplatné). Pokud licence *WinRoute* neobsahuje předplatné pro tento modul, chová se modul jako zkušební verze (po 30 dnech od instalace *WinRoute* se automaticky vypne a volby v záložce *Kerio Web Filter* budou neaktivní). Podrobné informace o licencích naleznete v kapitole 4.

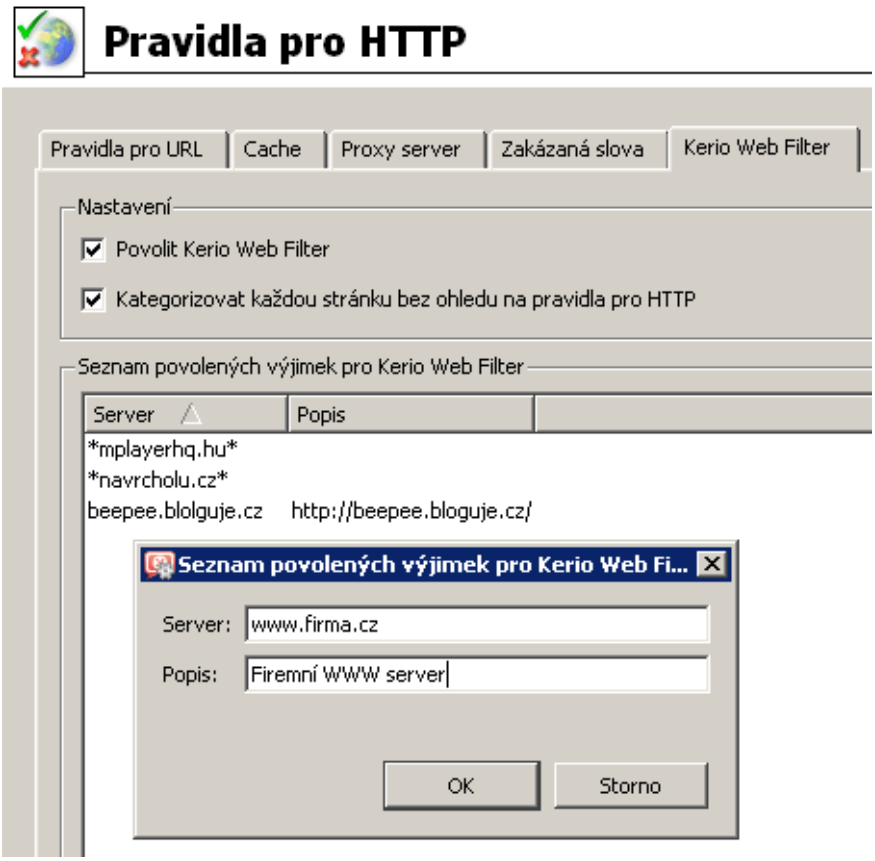
Nastavení parametrů modulu Kerio Web Filter

K aktivaci/deaktivaci a nastavení upřesňujících parametrů modulu *Kerio Web Filter* slouží záložka *Kerio Web Filter* v sekci *Konfigurace* → *Filtrování obsahu* → *Pravidla pro HTTP*.

Povolit Kerio Web Filter

Tato volba zapíná/vypíná modul pro klasifikaci WWW stránek *Kerio Web Filter*.
Je-li modul *Kerio Web Filter* vypnut, pak:

- nejsou dostupné ostatní volby v záložce *Kerio Web Filter*,
- jsou deaktivována všechna pravidla pro URL, která používají klasifikaci modulem *Kerio Web Filter* (podrobnosti viz kapitola 12.3).



Obrázek 12.6 Nastavení parametrů modulu Kerio Web Filter

Kategorizovat každou stránku bez ohledu ...

Po zapnutí této volby budou modulem *Kerio Web Filter* kategorizovány všechny WWW stránky (resp. všechny HTTP požadavky zpracované inspekčním modulem protokolu *HTTP*).

Kategorizace všech stránek je nutná pro sledování statistik kategorií navštívených stránek (viz kapitola 21). Nechceme-li tyto statistiky sledovat, doporučuje se tuto volbu vypnout (kategorizace všech stránek by zbytečně snižovala výkon *WinRoute*).

V poli *Výjimky pro Kerio Web Filter* lze specifikovat servery (případně konkrétní stránky), které nebudou tímto modulem kategorizovány. Tlačítko *Přidat* otevírá dialog pro zadání nové položky (serveru nebo stránky).

Server

Položka *Server* slouží ke specifikaci stránek, které nemají být klasifikovány modulem *Kerio Web Filter*. Do této položky lze zadat:

- jméno serveru (např. `www.kerio.cz`). Jméno serveru má význam libovolné stránky na tomto serveru,
- adresu konkrétní stránky bez specifikace protokolu (`http://`) — např. `www.kerio.cz/index.html`,
- masku URL s použitím hvězdičkové konvence (např. `*.ker?o.*`). Hvězdička na-

hrazuje libovolný (i nulový) počet znaků, otazník právě jeden znak.

Popis

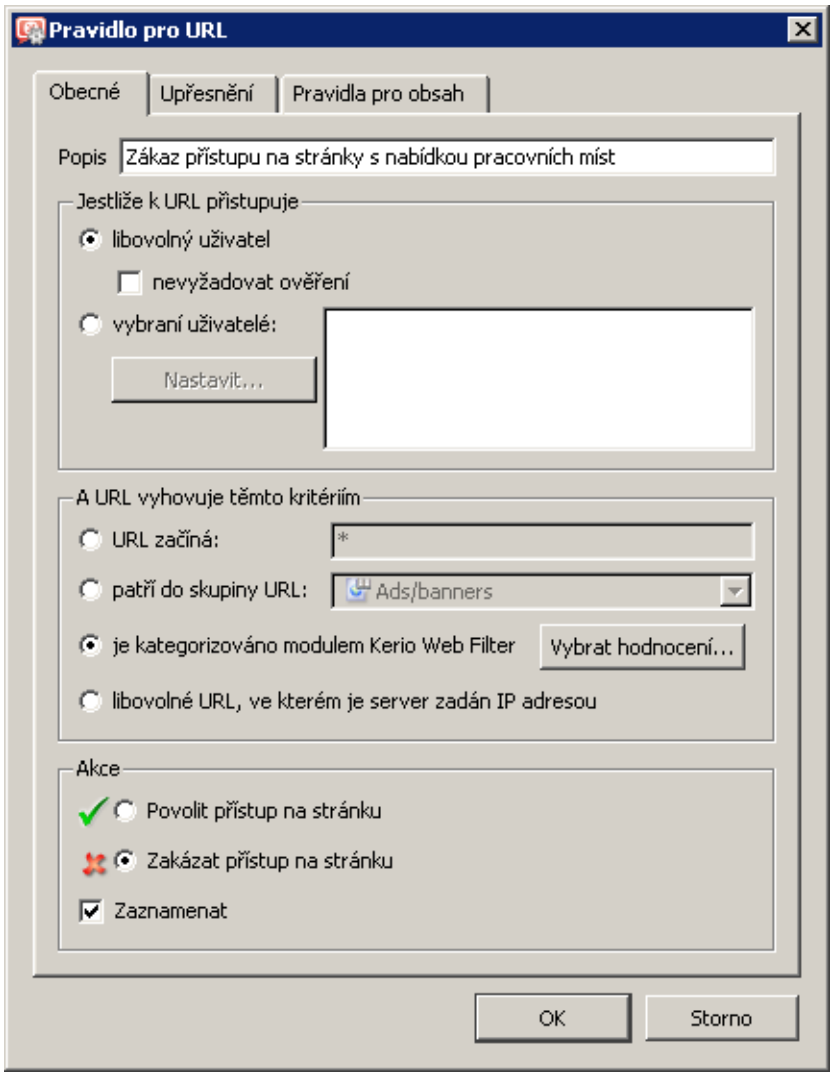
Textový popis definované výjimky. Slouží k lepší orientaci, není nutné jej vyplňovat.

Použití modulu Kerio Web Filter

Pro klasifikaci WWW stránek modulem *Kerio Web Filter* musí být tento modul zapnut a nastaveny jeho parametry.

Modul *Kerio Web 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.

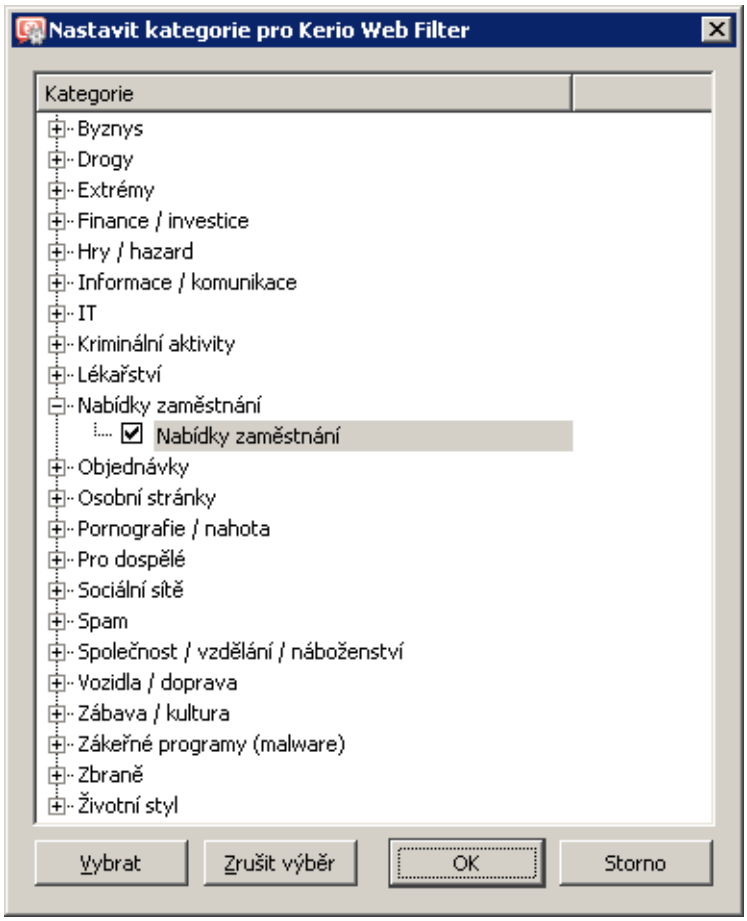
V sekci *Konfigurace* → *Filtrování obsahu* → *Pravidla pro HTTP*, záložka *Pravidla pro URL*, definujeme pravidlo dle obrázku 12.7.



Obrázek 12.7 Pravidlo pro filtrování WWW stránek dle kategorií systému Kerio Web Filter

Klíčovým parametrem je volba *je kategorizováno modulem Kerio Web Filter*. URL každé navštívené stránky bude klasifikováno, a bude-li zařazeno do některé z vybraných kategorií, pak *WinRoute* zakáže přístup na tuto stránku.

Tlačítkem *Vybrat hodnocení* otevřeme dialog pro výběr kategorií modulu *Kerio Web Filter* a zvolíme kategorii *Zaměstnání / Nabídky zaměstnání* (stránky s nabídkami pracovních míst).



Obrázek 12.8 Výběr kategorií systému Kerio Web Filter

Poznámka:

1. Pravidel pro URL využívajících *Kerio Web Filter* může být definováno více. V každém pravidle může být nastaveno více kategorií.

2. V pravidlech používajících klasifikaci modulem *Kerio Web Filter* je vhodné povolit odemknutí (záložka *Upřesnění*, volba *Uživatelé mohou toto pravidlo "odemknout"*) — pro případ, že bude stránka blokována z důvodu nesprávné klasifikace. Všechny požadavky na odemknutí pravidel se zaznamenávají do záznamu *Filter* — zde můžeme zkontrolovat, zda byl požadavek uživatele oprávněný či nikoliv.

12.4 Filtrování WWW stránek dle výskytu slov

WinRoute může filtrovat WWW stránky podle výskytu nežádoucích slov.

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 (tzv. prahovou hodnotu), stránka je blokována.

Pro účely filtrování WWW stránek dle nežádoucích slov umožňuje *WinRoute* definovat tzv. zakázaná slova. Pomocí pravidel pro URL (viz kapitola 12.2) lze pak definovat podmínky, za kterých bude filtrování stránek obsahujících zakázaná slova prováděno.

Upozornění

Bez příslušných pravidel pro URL nemá definice zakázaných slov a prahové hodnoty žádný smysl!

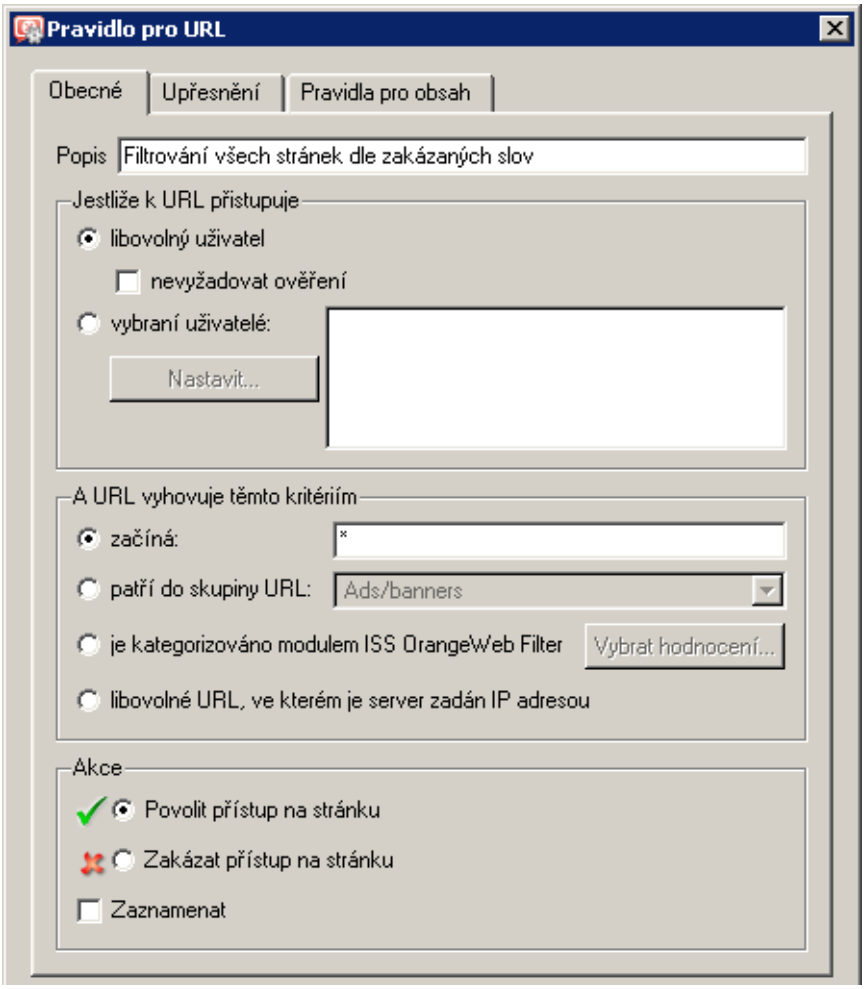
Definice pravidel pro filtrování dle výskytu slov

Předpokládejme, že jsou již definována nějaká zakázaná slova a je nastavena prahová hodnota váhy stránky (podrobnosti viz dále).

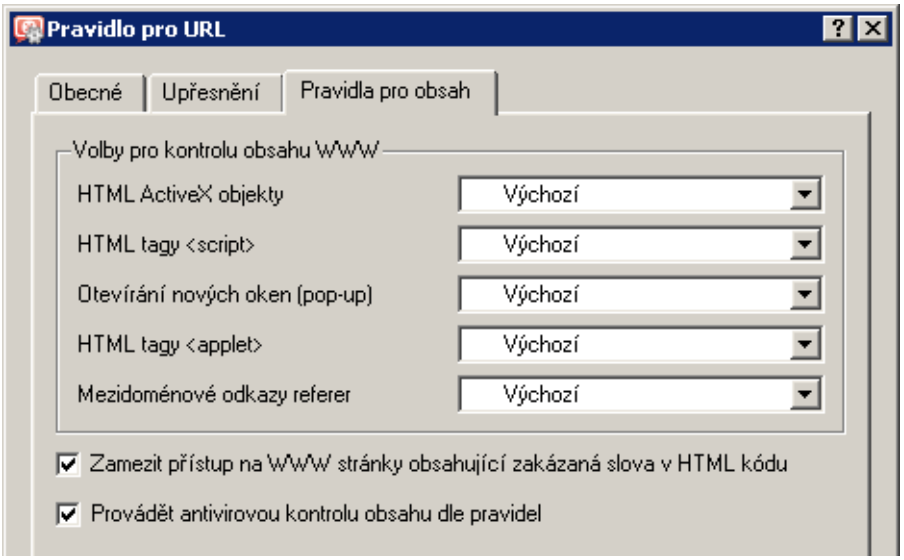
V záložce *Pravidla pro URL* sekce *Konfigurace* → *Filtrování obsahu* → *Pravidla pro HTTP* vytvoříme pravidlo (případně více pravidel) povolující přístup ke skupině stránek, které mají být filtrovány dle zakázaných slov. V záložce *Pravidla pro obsah* aktivujeme filtrování stránek obsahujících zakázaná slova.

Jako příklad uvedeme definici pravidla pro filtrování všech WWW stránek dle výskytu zakázaných slov:

- V záložce *Obecné* povolíme přístup všem uživatelům ke všem WWW stránkám.
- V záložce *Pravidla pro obsah* zapneme volbu *Zamezit přístup na WWW stránky obsahující...*, která aktivuje filtrování dle zakázaných slov.



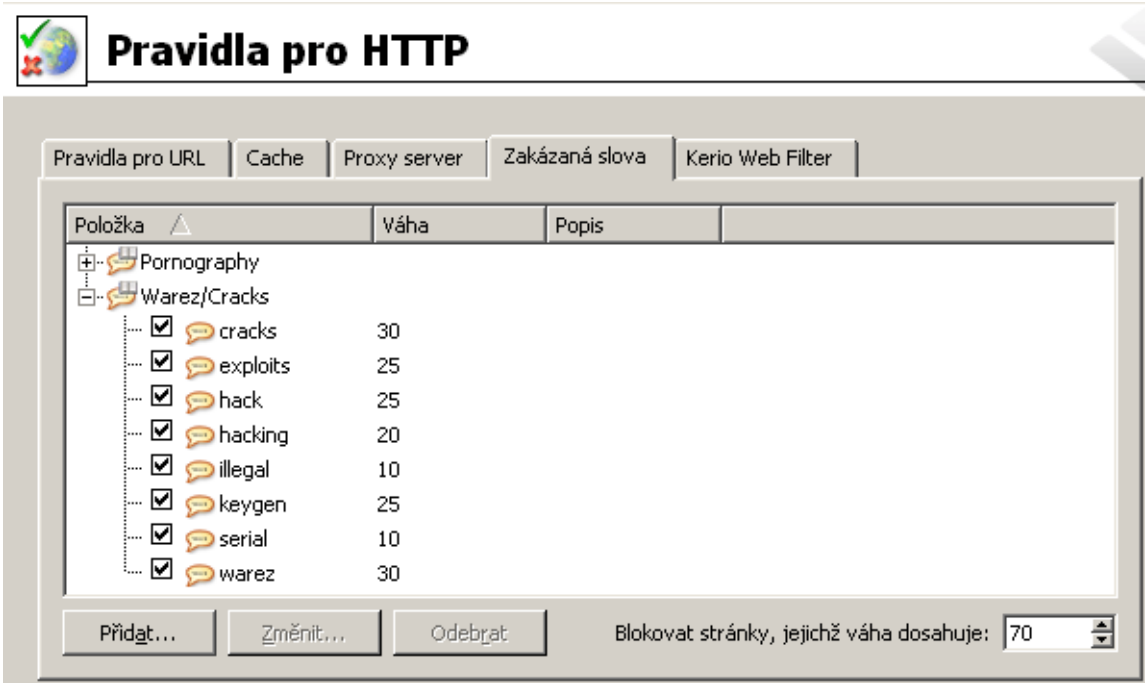
Obrázek 12.9 Pravidlo pro filtrování WWW stránek dle výskytu slov (povolení přístupu)



Obrázek 12.10 Pravidlo pro filtrování WWW stránek dle výskytu slov (filtrování slov)

Skupiny slov

K definici skupin slov slouží záložka *Skupiny slov* v sekci *Konfigurace* → *Filtrování obsahu* → *Pravidla pro HTTP*. Jednotlivá slova se pro přehlednost řadí do skupin. Zařazení do skupiny nemá žádný vliv na filtrování — vždy se testují všechna slova ze všech skupin.



Obrázek 12.11 Skupiny zakázaných slov

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 / Cracks* — slova, která obvykle obsahují stránky nabízející ke stažení nelegální software, generátory licenčních klíčů apod.

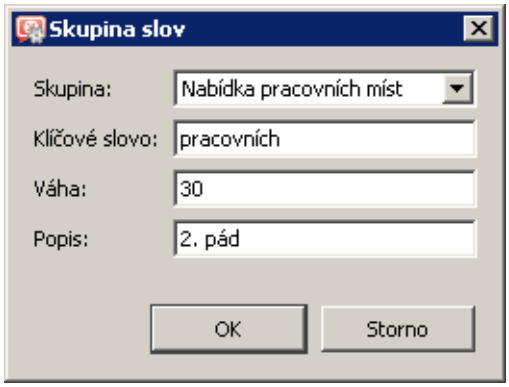
Všechna slova v předdefinovaných skupinách jsou ve výchozím nastavení „vypnuta“. Správce *WinRoute* je může použít a upravit jejich váhu dle vlastního uvážení.

Prahová hodnota pro blokování WWW stránek

Volba *Blokovat stránky, jejichž váha je vyšší než* určuje tzv. prahovou hodnotu 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).

Definice zakázaných slov

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



Obrázek 12.12 Definice zakázaného slova a/nebo skupiny slov

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. Slovo může být v jakémkoliv jazyce a mělo by být zapsáno přesně ve tvaru, v jakém se na WWW stránkách vyskytuje (s použitím příslušných národních znaků apod.). Má-li slovo více tvarů (jednotné/množné číslo, pády podstatných jmen apod.), je potřeba pro každý tvar definovat samostatné slovo v dané skupině. Jednotlivé tvary slova mohou mít i různé váhy.

Váha
: Váha slova je míra vlivu slova na blokaci přístupu na stránku. Nastavená váha by měla zohledňovat četnost výskytu daného slova v příslušném jazyce (čím běžnější slovo, tím nižší váha), aby nedocházelo k blokování stránek s nezávadných obsahem.

Popis
: Libovolný textový komentář (pro přehlednost).

12.5 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).

Obrázek 12.13 Pravidla pro FTP

Poznámka:

1. 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.

2. Ve výchozím nastavení je zapnuto pravidlo zakazující pokračování ve stahování souboru po přerušení (tzv. *resume* — FTP příkaz `REST`). Toto je velmi důležité pro správnou funkci antivirové kontroly: pro spolehlivé nalezení viru je třeba, aby byl soubor kontrolován jako celek.

   Je-li toto chování nežádoucí, můžeme předdefinované pravidlo vypnout. Pak ale není zaručena plná spolehlivost antivirové kontroly. Bezpečnější postup v takovém případě je definovat výjimku pro konkrétní FTP server — pravidlo povolující přístup na tento server bez omezení. Toto pravidlo musí být umístěno nad předdefinovaným pravidlem zakazujícím pokračování ve stahování.

   Podrobnosti o antivirové kontrole protokolu FTP naleznete v kapitole 13.3.

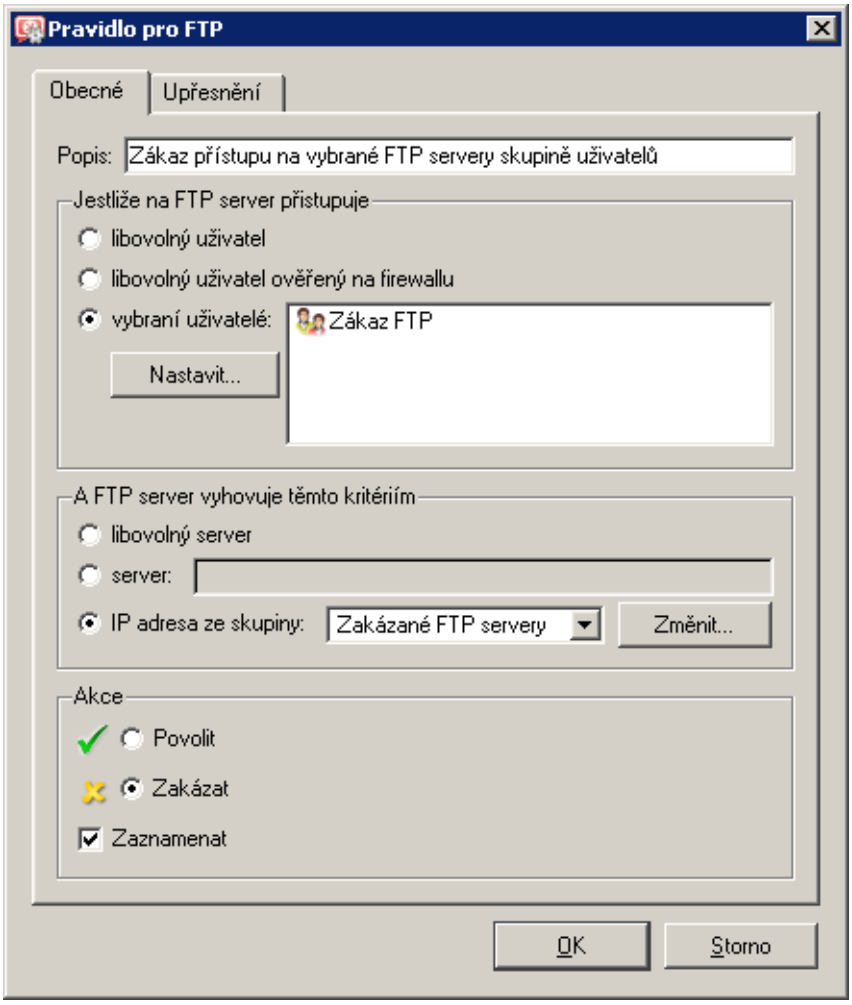
Definice pravidel pro FTP

Chceme-li přidat nové pravidlo, označíme v tabulce pravidlo, pod které má být nové pravidlo vloženo, a stiskneme tlačítko *Přidat*. Šipkovými tlačítky na pravé straně okna lze pořadí pravidel dodatečně upravit.

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.

Dialog pro definici pravidla pro FTP:



Obrázek 12.14 Pravidlo pro FTP — základní parametry

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 pří-

stup nepřihlášeným uživatelům.

A FTP server vyhovuje těmto kritériím

Specifikace FTP serverů, pro které má toto pravidlo platit:

- *libovolný server* — libovolný FTP server
- *server* — IP adresa nebo DNS jméno konkrétního FTP serveru.
  Je-li FTP server zadán DNS jménem, pak *WinRoute* automaticky zjistí z DNS odpovídající IP adresu. Zjištění IP adresy se provádí bezprostředně po potvrzení změn stisknutím tlačítka *Použít* (pro všechna pravidla, v nichž byl FTP server zadán jménem).

  Upozornění

  Dokud se nepodaří zjistit odpovídající IP adresu, je příslušné pravidlo neaktivní!
- *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 14.1).

Akce

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

- *Povolit* — *WinRoute* povolí přístup na definované FTP servery za podmínek nastavených v záložce *Upřesnění* — viz dále).
- *Zakázat* — *WinRoute* bude blokovat určité FTP příkazy či celé spojení (v závislosti na nastavení v záložce *Upřesnění*).

Zaškrtnutím volby *Zaznamenat* budou všechny přístupy na FTP, které vyhověly tomuto pravidlu, zaznamenány do záznamu *Filter* (viz kapitola 22.9).

V záložce *Upřesnění* jsou obsaženy další podmínky, za kterých má pravidlo platit, a upřesňující podmínky 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 14.2).

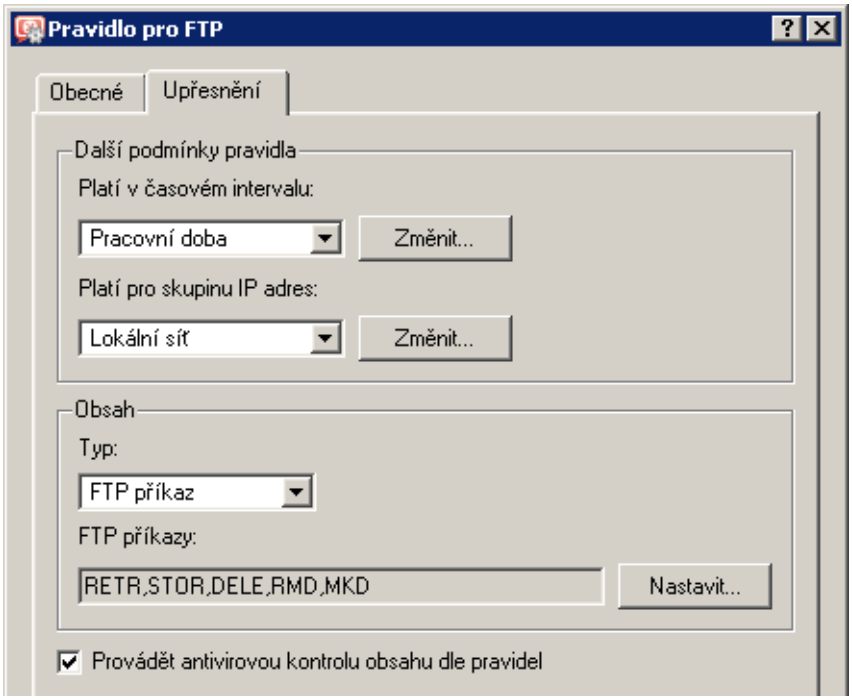
Platí pro skupinu IP adres

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 14.1).

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.



Obrázek 12.15 Pravidlo pro FTP — upřesňující nastavení

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

Provádět antivirovou kontrolu obsahu dle pravidel

Zapnutí/vypnutí antivirové kontroly FTP komunikace vyhovující tomuto pravidlu.

Tato volba je dostupná pouze v povolujících pravidlech — je-li určitá komunikace zakázána, nemá nastavení antivirové kontroly smysl.

Kapitola 13

Antivirová kontrola

WinRoute umožňuje kontrolovat antivirovým programem objekty (soubory) přenášené protokoly HTTP, FTP, SMTP a POP3. V případě protokolů HTTP a FTP může správce *WinRoute* specifikovat, které objekty (resp. typy objektů) mají být kontrolovány.

WinRoute je dodáván s integrovaným antivirem *McAfee* (jeho použití vyžaduje speciální licenci). Kromě integrovaného modulu *WinRoute* podporuje externí antiviry různých dalších výrobců. 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 umožňuje použít současně integrovaný antivirový modul *McAfee* a zvolený externí antivirus. Přenášené soubory jsou pak kontrolovány oběma antiviry (tzv. duální antivirová kontrola). Tím se snižuje pravděpodobnost propuštění souboru s virem.

Současné použití dvou antivirů má však negativní dopad na výkon firewallu. Doporučujeme proto důkladně zvážit, zda duální antivirovou kontrolu použít a na jaké protokoly ji aplikovat, případně provést testy se zkušební verzí *WinRoute* před zakoupením příslušné licence.

Poznámka:

1. Podporované externí antiviry, stejně jako verze jednotlivých programů a obchodní podmínky, se mohou v průběhu času měnit. Aktuální informace vždy naleznete na WWW stránkách firmy *Kerio Technologies* (http://www.kerio.cz/cz/firewall).

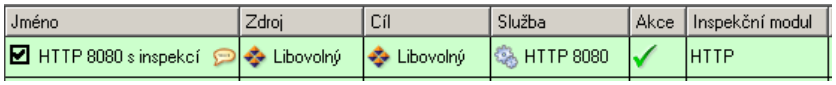
2. Externí *McAfee Anti-Virus* není ve *WinRoute* podporován.

13.1 Podmínky a omezení antivirové kontroly

Antivirovou kontrolu objektů přenášených určitým protokolem lze provádět pouze v případě, že je komunikace sledována příslušným inspekčním modulem (viz kapitola 14.3) a tento modul podporuje spolupráci s antivirem. Z toho vyplývají následující omezení:

- Antivirovou kontrolu nelze provádět při použití zabezpečeného kanálu (SSL/TLS). V tomto případě není technicky možné dešifrovat komunikaci a oddělit jednotlivé přenášené objekty.
- Při antivirové kontrole e-mailu (protokoly SMTP a POP3) firewall pouze odstraňuje infikované přílohy — není možné zahazovat celé zprávy. V případě protokolu SMTP se standardně kontroluje pouze příchozí komunikace (tzn. z Internetu do lokální sítě — příchozí pošta na lokální SMTP server). Kontrola odchozí komunikace způsobuje problémy při dočasných chybách doručení.
  Podrobnosti viz kapitola 13.4.

- Objekty přenášené jinými protokoly než HTTP, FTP, SMTP a POP3 nelze kontrolovat antivirem.
- Je-li při komunikaci použit nestandardní port, pak nebude příslušný inspekční modul aplikován automaticky. V tomto případě stačí definovat komunikační pravidlo povolující tuto komunikaci s použitím příslušného inspekčního modulu (podrobnosti viz kapitola 7.3).
  Příklad: Chceme provádět antivirovou kontrolu protokolu HTTP na portu 8080.
  1. Definujeme službu *HTTP 8080* (protokol TCP, port 8080).
  2. Vytvoříme komunikační pravidlo povolující tuto službu s použitím příslušného inspekčního modulu.



Obrázek 13.1 Komunikační pravidlo pro inspekci protokolu HTTP na nestandardním portu

  Vytvořené pravidlo umístíme nad pravidlo povolující přístup do Internetu k libovolné službě (pokud je takové pravidlo definováno). V případě, že je pro přístup do Internetu použita technologie NAT (překlad zdrojových IP adres), musíme v tomto pravidle rovněž nastavit překlad adres.
  Poznámka: Inspekční modul můžeme rovněž uvést v definici služby, případně na obou místech — efekt je ve všech případech stejný (při uvedení přímo v komunikačním pravidle je však pravidlo „průhlednější“).

13.2 Výběr a nastavení antivirových programů

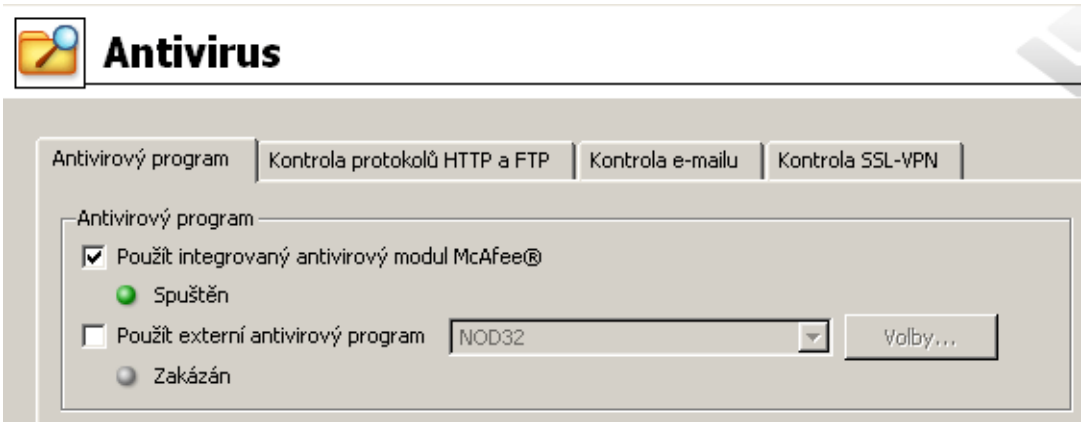
K výběru antivirových programů a nastavení jejich parametrů slouží sekce *Konfigurace* → *Filtrování obsahu* → *Antivirus*, záložka *Antivirový program*. V této záložce můžeme zvolit integrovaný modul *McAfee*, externí antivirový program nebo oba současně.

Budou-li použity oba antiviry, pak bude každý přenášený objekt (stahovaný soubor, příloha e-mailové zprávy atd.) zkontrolován nejprve integrovaným modulem *McAfee* a poté zvoleným externím antivirem.

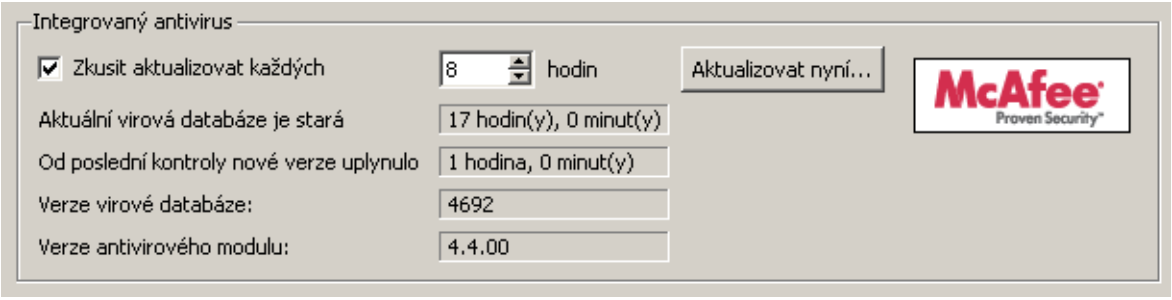
Integrovaný antivirus McAfee

Chceme-li použít integrovaný antivirus *McAfee*, zapneme v horní části záložky *Antivirový program* volbu *Použít Integrovaný antivirový modul McAfee*. Tato volba je dostupná pouze v případě, že licenční klíč *WinRoute* obsahuje licenci pro antivirový modul *McAfee*, nebo jedná-li se o zkušební verzi *WinRoute*. Podrobné informace o licencích naleznete v kapitole 4.

V dolní části záložky *Antivirový program* je nyní aktivní sekce *Integrovaný antivirový modul*, ve které lze nastavit aktualizaci modulu *McAfee*.



Obrázek 13.2 Výběr antivirového programu (integrovaný antivirový modul)



Obrázek 13.3 Nastavení aktualizace integrovaného antivirového modulu McAfee

Zkusit aktualizovat každých ... hodin

Tato volba zapíná/vypíná automatickou kontrolu nových verzí virové databáze a antivirového programu v nastaveném intervalu.

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 22.8).

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

Upozornění

Pro zajištění maximální účinnosti antivirové kontroly je nutné, aby měl antivirový modul vždy k dispozici nejnovější verzi virové databáze. Z tohoto důvodu doporučujeme nevypínat automatickou aktualizaci a nenastavovat příliš velké intervaly pokusů o aktualizaci (pokus o aktualizaci by měl proběhnout alespoň dvakrát denně).

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.

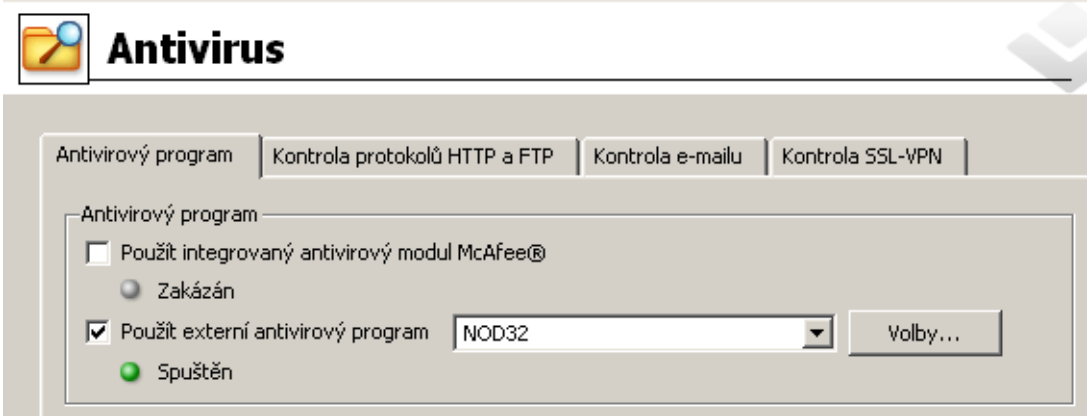
Verze antivirového modulu
Číslo verze antivirového modulu *McAfee*, který *WinRoute* používá.

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 pokusu o aktualizaci. 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*.

Externí antivirový program

Chceme-li použít některý z podporovaných externích antivirů, zapneme volbu *Použít externí antivirový program* v horní části záložky *Antivirový program* a vybereme požadovaný antivirus. Nabídka obsahuje všechny antivirové programy, které *WinRoute* podporuje pomocí speciálních modulů (*plugins*).

Upozornění
Externí antivirový program musí být nainstalován dříve, než bude ve *WinRoute* nastaven. Před instalací antivirového programu doporučujeme zastavit službu *WinRoute Firewall Engine*.



Obrázek 13.4 Výběr antivirového programu (externí antivirus)

Tlačítko *Volby* otevírá dialog pro nastavení upřesňujících parametrů vybraného antivirového programu. Tyto parametry jsou závislé na konkrétním antiviru (pro některé antiviry nelze, resp. není třeba nastavovat žádné parametry). Podrobné informace o instalaci a konfiguraci jednotlivých antivirových programů naleznete na adrese http://www.kerio.cz/cz/firewall/third-party.

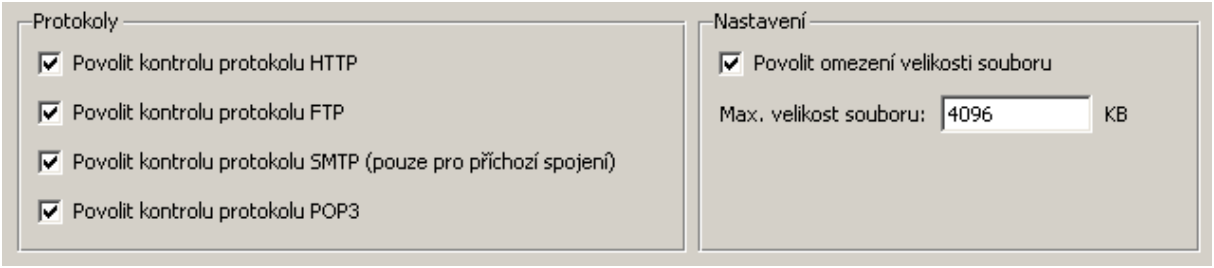
Po stisknutí tlačítka *Použít* se provede test vybraného antiviru. Je-li test úspěšný, bude tento antivirus nadále používán. Je-li test neúspěšný, zobrazí se chybové hlášení a zůstane nastaven předchozí antivirus. Do záznamu *Error* (viz kapitola 22.8) se zapíší podrobné informace o zjištěné chybě.

Nastavení parametrů antivirové kontroly

V poli *Protokoly* záložky *Antivirový program* lze zvolit aplikační protokoly, na které bude antivirová kontrola aplikována. Ve výchozím nastavení je antivirová kontrola zapnuta pro všechny podporované protokoly.

V poli *Nastavení* lze určit maximální velikost souborů, které budou antivirem na firewallu kontrolovány. Kontrola velkých souborů je náročná na čas, procesor i diskový prostor serveru, což může mít zásadní negativní vliv na činnost firewallu. V některých případech může také dojít k přerušení spojení, kterým je soubor přenášen, z důvodu vypršení časového limitu.

Optimální hodnota je závislá na konkrétních podmínkách (výkon serveru, intenzita síťového provozu, charakter přenášených dat, typ použitého antiviru atd.). *Důrazně doporučujeme neměnit výchozí nastavení omezení velikosti souboru, v žádném případě nenastavovat vyšší hodnotu než výchozí (4 MB).*



Obrázek 13.5 Výběr kontrolovaných aplikačních protokolů a omezení velikosti souboru

Parametry kontroly protokolů HTTP a FTP lze nastavit v záložce *Kontrola HTTP a FTP* (viz kapitola 13.3), parametry kontroly SMTP a POP3 v záložce *Kontrola e-mailu* (viz kapitola 13.4).

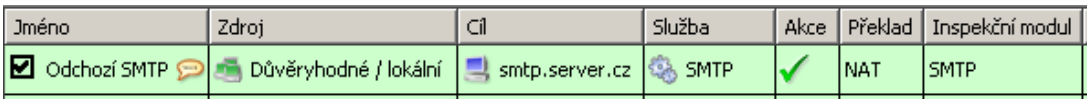
Upozornění

1. V případě protokolu SMTP se standardně provádí pouze kontrola příchozí komunikace (tj. komunikace z Internetu do lokální sítě — příchozí pošta na lokální SMTP server). Kontrola odchozí SMTP komunikace (z lokální sítě do Internetu) by mohla způsobovat problémy při dočasných chybách doručení — typicky pokud cílový SMTP server používá tzv. *greylisting*.

   Chceme-li kontrolovat rovněž odchozí komunikaci, je třeba definovat odpovídající komunikační pravidlo s použitím inspekčního modulu protokolu SMTP. Toto může být užitečné

např. v případě, kdy klienti v lokální síti odesílají poštu přes SMTP server v Internetu. Kontrola odchozí SMTP komunikace není vhodná pro lokální SMTP server, který odesílá poštu do Internetu.

Příklad komunikačního pravidla pro kontrolu odchozí SMTP komunikace je uveden na obrázku 13.6.



Obrázek 13.6 Příklad komunikačního pravidla pro kontrolu odchozí SMTP komunikace

2. Při vzájemné komunikaci dvou poštovních serverů *Microsoft Exchange* mohou být použita nestandardní rozšíření protokolu SMTP. E-mailové zprávy se v některých případech přenášejí v binární podobě. *WinRoute* pak nemůže provádět antivirovou kontrolu jednotlivých příloh.

   V těchto případech doporučujeme použít antivirový program, který spolupracuje přímo s *Microsoft Exchange*, a ve *WinRoute* neprovádět kontrolu SMTP komunikace příslušného serveru. Toho lze docílit buď vypnutím antivirové kontroly protokolu SMTP nebo definicí odpovídajícího komunikačního pravidla bez použití inspekčního modulu (viz kapitola 7.7).

13.3 Antivirová kontrola protokolů HTTP a FTP

V případě protokolů HTTP a FTP se provádí kontrola přenášených objektů (souborů) zvolených typů.

Přenášený soubor je zároveň ukládán do dočasného adresáře na lokálním disku firewallu. Poslední část souboru (blok přenášených dat) *WinRoute* pozdrží ve své vyrovnávací paměti a provede antivirovou kontrolu souboru v dočasném adresáři. Je-li v souboru nalezen virus, pak *WinRoute* poslední blok dat zahodí. Klient tak dostane soubor poškozený (neúplný) — nebude jej moci spustit a virus aktivovat. Není-li nalezen žádný virus, pak *WinRoute* pošle klientovi zbývající část souboru a přenos je úspěšně dokončen.

Uživateli, který soubor stahoval, může být volitelně zaslána výstraha o nalezeném viru (viz volba *Upozornit klienta*).

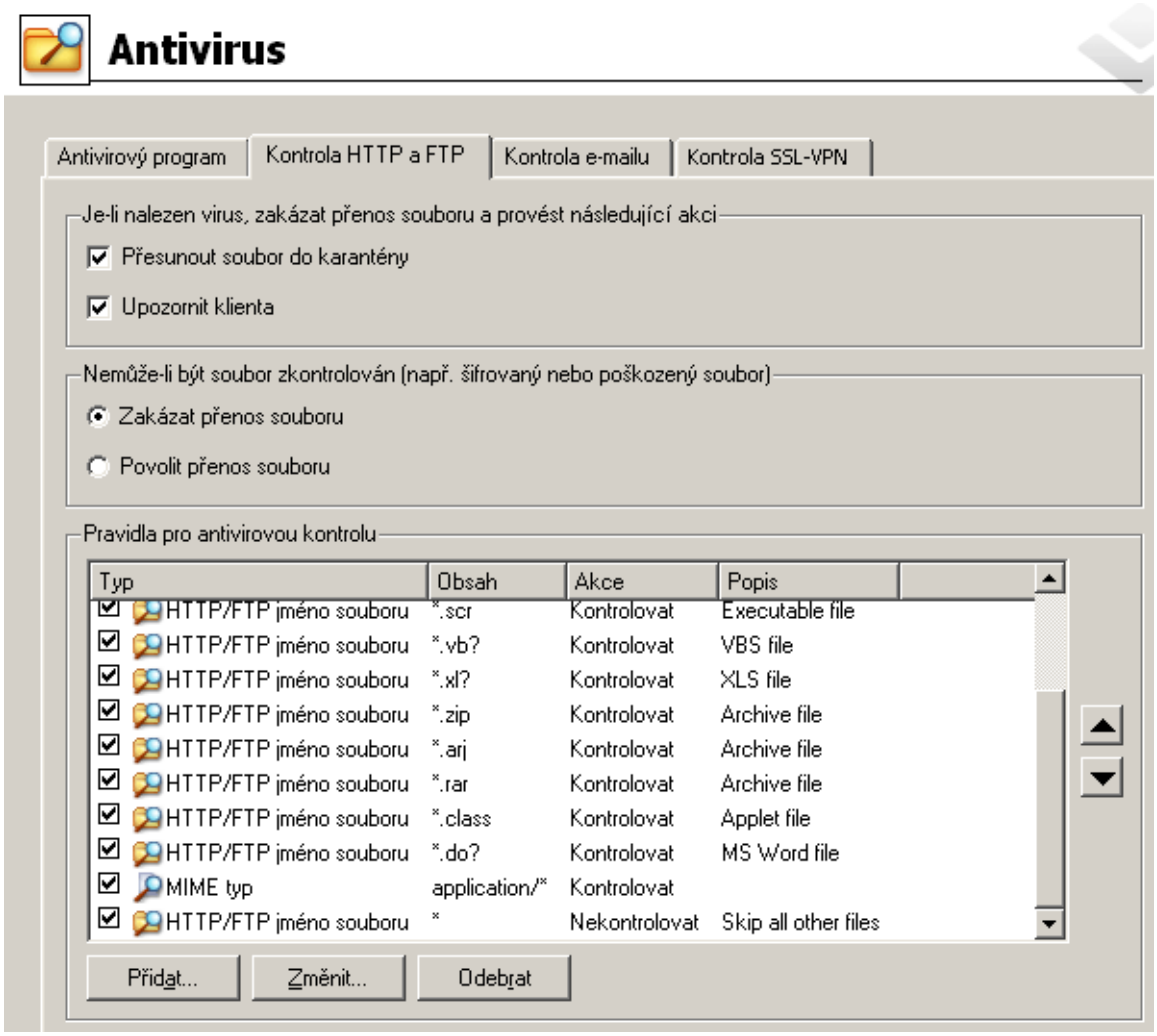
Upozornění

1. Antivirová kontrola dokáže pouze nalézt a blokovat infikované soubory, není možné je léčit!

2. V pravidlech pro filtrování protokolů HTTP a FTP může být antivirová kontrola vypnuta — pak se nekontrolují objekty a soubory vyhovující příslušnému pravidlu. Podrobnosti naleznete v kapitolách 12.2 a 12.5.

3. Při použití nestandardních rozšíření WWW prohlížečů (od jiných výrobců — typicky download managery, akcelerátory apod.) není zaručena plná funkčnost antivirové kontroly protokolu HTTP!

Parametry kontroly protokolů HTTP a FTP lze nastavit v sekci *Konfigurace* → *Filtrování obsahu* → *Antivirus*, záložka *Kontrola HTTP a FTP*.



Obrázek 13.7 Nastavení antivirové kontroly protokolů HTTP a FTP

V poli *Je-li nalezen* virus lze specifikovat akce, které budou provedeny při detekci viru v přenášeném souboru:

- *Přesunout soubor do karantény* — soubor bude uložen do speciálního adresáře na počítači s *WinRoute*. Správce *WinRoute* se pak může pokusit tento soubor léčit antivirovým programem a v případě úspěchu pak předat uživateli, který jej stahoval.
  Pro karanténu se používá podadresář `quarantine` v adresáři *WinRoute* (typicky `C:\Program Files\Kerio\WinRoute Firewall\quarantine`).
  Infikované (resp. podezřelé) soubory jsou do tohoto adresáře ukládány pod automaticky vytvořenými jmény. Jméno každého souboru obsahuje protokol, datum, čas a číslo spojení, kterým byl soubor přenášen.

Upozornění

Při práci se soubory v adresáři `quarantine` je třeba dbát zvýšené opatrnosti, aby nedošlo k aktivaci některého viru a infikaci počítače s *WinRoute*!

- *Upozornit klienta* — *WinRoute* pošle uživateli, který tento soubor stahoval, e-mailovou zprávu s výstrahou, že v tomto souboru byl detekován virus a stahování bylo přerušeno.
  Výstrahu *WinRoute* vyšle pouze za těchto podmínek: uživatel je přihlášen na firewall, v příslušném uživatelském účtu je nastavena platná e-mailová adresa (viz kapitola 15.1) a je korektně nastaven SMTP server pro odesílání pošty (viz kapitola 18.3).
  Poznámka: Nezávisle na volbě *Upozornit klienta* lze při detekci virů zasílat výstrahy na definované adresy (např. správcům sítě). Podrobnosti naleznete v kapitole 19.4.

Pole *Nemůže-li být soubor zkontrolován* umožňuje nastavit akci pro případy, kdy nelze provést antivirovou kontrolu přenášeného souboru (např. komprimovaný soubor chráněný heslem, poškozený soubor atd.):

- *Zakázat přenos souboru* — *WinRoute* bude tyto soubory považovat za infikované a nepovolí jejich přenos.

  Tip

  Tuto volbu je vhodné kombinovat s volbou *Přesunout soubor do karantény* — správce *WinRoute* může pak např. ve spolupráci s příslušným uživatelem soubor dekomprimovat a provést antivirovou kontrolu ručně.

- *Povolit přenos souboru* — *WinRoute* bude předpokládat, že šifrované či poškozené soubory neobsahují viry.
  Tato volba obecně není bezpečná, ale lze ji využít např. v případě, kdy uživatelé přenášejí velké množství šifrovaných souborů (archivů) a na pracovních stanicích je nainstalován antivirový program.

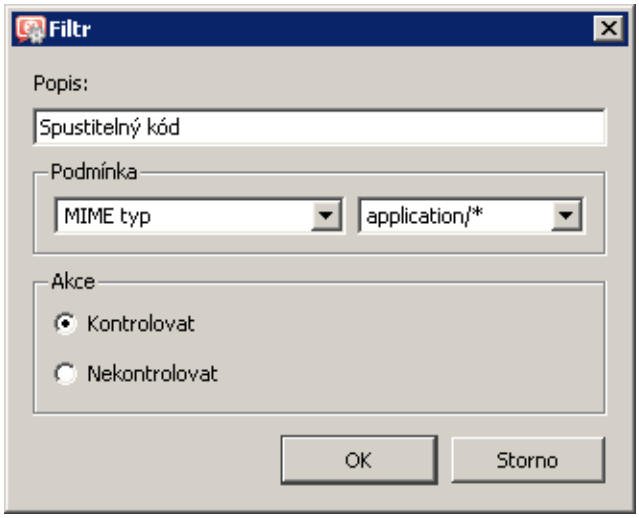
Pravidla pro antivirovou kontrolu HTTP a FTP

Tato pravidla slouží k nastavení podmínek, za kterých má být antivirová kontrola prováděna. Implicitně (tj. pokud není definováno žádné pravidlo) se kontrolují všechny objekty přenášené protokoly HTTP a FTP.

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

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.



Obrázek 13.8 Definice pravidla pro antivirovou kontrolu protokolů HTTP a FTP

Popis

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

Podmínka

Podmínka pravidla:

- *HTTP/FTP jméno souboru*
  Volbou lze filtrovat jména souborů (nikoli celá URL) přenášených protokolem FTP nebo HTTP (např. `*.exe`, `*.zip` atd.).
  Zadáme-li jako jméno souboru pouze hvězdičku, bude pravidlo platit pro všechny soubory přenášené protokoly HTTP a FTP.

Zbývající podmínky lze aplikovat pouze na protokol HTTP:

- *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/*`).

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

Akce

Volba, zda objekt má či nemá být kontrolován antivirovým programem.
Volba *Nekontrolovat* znamená, že přenos objektu bude povolen bez antivirové kontroly.

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.

Nevyhoví-li objekt žádnému pravidlu, pak je antivirovým programem automaticky zkontrolován. Mají-li být kontrolovány pouze vybrané typy objektů, musí být na konci seznamu uvedeno pravidlo zakazující antivirovou kontrolu pro libovolné URL či libovolný MIME typ (předdefinované pravidlo *Skip all other files*).

13.4 Antivirová kontrola e-mailu

Záložka *Kontrola e-mailu* umožňuje nastavit parametry antivirové kontroly protokolů SMTP a POP3. Je-li antivirová kontrola pro tyto protokoly (resp. některý z nich) zapnuta, pak se kontrolují všechny přílohy všech přenášených zpráv.

Jednotlivé přílohy přenášené zprávy *WinRoute* postupně ukládá do dočasného adresáře na lokálním disku. Po uložení celého souboru provede antivirovou kontrolu. Není-li nalezen virus, je příloha vložena zpět do zprávy. Při nalezení viru je příloha nahrazena textovou informací o nalezeném viru.

Poznámka: Při detekci virů lze rovněž zasílat výstrahy na definované adresy (např. správcům sítě). Podrobnosti naleznete v kapitole 19.4.

Upozornění

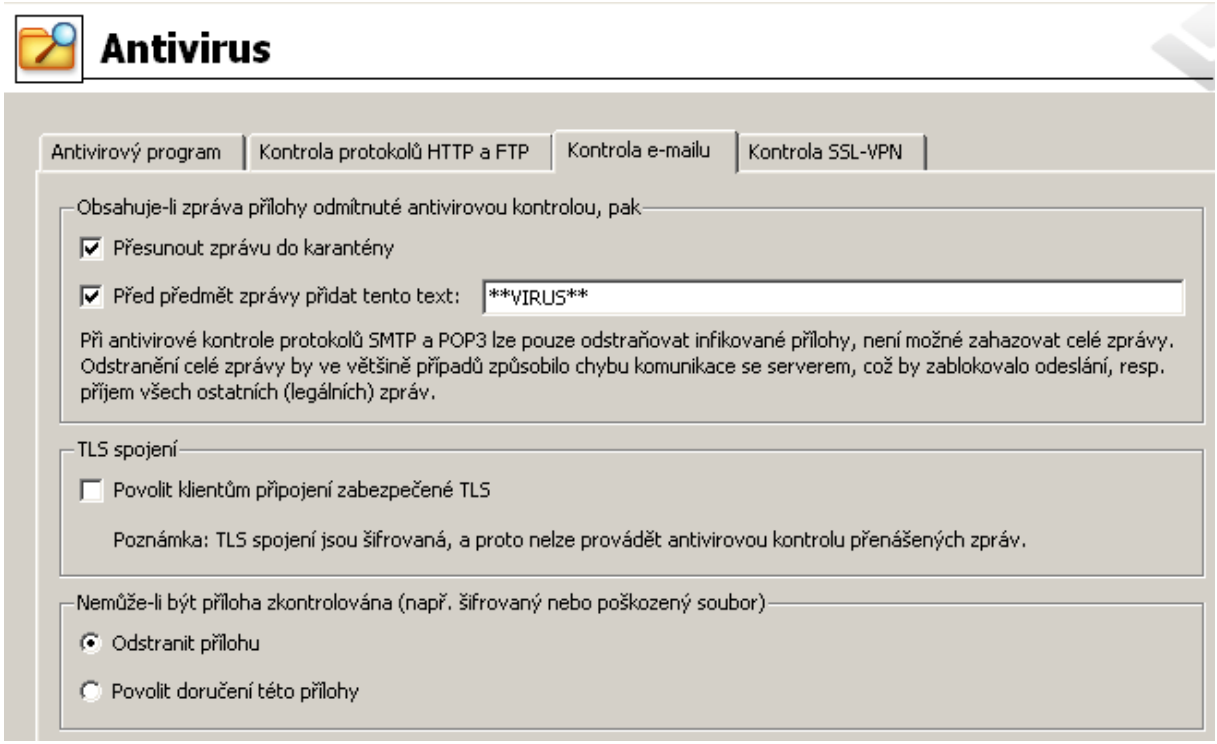
1. Antivirová kontrola e-mailové komunikace dokáže pouze nalézt a blokovat infikované přílohy zpráv. Přílohy není možné léčit!

2. Při antivirové kontrole e-mailu lze pouze odstraňovat infikované přílohy, není možné zahazovat celé zprávy. Důvodem je, že firewall nepracuje se zprávami jako poštovní server, ale jen zasahuje do síťové komunikace, která přes něj prochází. Odstranění celé zprávy by ve většině případů způsobilo chybu komunikace se serverem a klient by se pravděpodobně pokusil odeslat, resp. stáhnout zprávu znovu. V důsledku by jedna zavirovaná zpráva zablokovala odeslání, resp. příjem všech ostatních (legitimních) zpráv.

3. V případě protokolu SMTP se standardně provádí pouze kontrola příchozí komunikace (tj. komunikace z Internetu do lokální sítě — příchozí pošta na lokální SMTP server). Kontrola odchozí SMTP komunikace (tj. z lokální sítě do Internetu) by mohla způsobovat problémy při dočasných chybách doručení (typicky pokud cílový SMTP server používá tzv. *greylisting*).

   Chceme-li kontrolovat rovněž odchozí komunikaci (např. pokud se lokální klienti připojují na SMTP server mimo lokální síť), je třeba definovat odpovídající komunikační pravidlo s použitím inspekčního modulu protokolu SMTP. Viz též kapitola 13.2.

Záložka *Antivirová kontrola e-mailu* umožňuje nastavit akce při nalezení viru a upřesňující parametry.



Obrázek 13.9 Nastavení antivirové kontroly protokolů SMTP a POP3

V poli *Obsahuje-li zpráva přílohy odmítnuté antivirovou kontrolou* lze nastavit akce pro zprávu, ve které byla nalezena alespoň jedna infikovaná příloha:

- *Přesunout zprávu do karantény* — zpráva bude uložena do speciálního adresáře na počítači s *WinRoute*. Správce *WinRoute* se pak může pokusit infikované přílohy léčit antivirovým programem a v případě úspěchu je předat původnímu adresátovi.
  Pro karanténu se používá podadresář `quarantine` v adresáři *WinRoute* (typicky `C:\Program Files\Kerio\WinRoute Firewall\quarantine`). Zprávy s infikovanými (resp. podezřelými) přílohami jsou do tohoto adresáře ukládány pod automaticky vytvořenými jmény. Jméno každého souboru obsahuje protokol, datum, čas a číslo spojení, kterým byla zpráva s infikovanou přílohou přenášena.
- *Před předmět zprávy přidat tento text* — touto volbou lze specifikovat text, který bude připojen před předmět každé e-mailové zprávy, ve které byla nalezena alespoň jedna infikovaná příloha. Tento text slouží pro upozornění příjemce zprávy a lze jej také použít k automatickému filtrování zpráv.

Poznámka: Bez ohledu na nastavenou akci, při detekci viru v příloze zprávy je tato příloha vždy ze zprávy odstraněna a nahrazena varováním.

V poli *TLS spojení* lze nastavit chování firewallu pro případy, kdy poštovní klient i server podporují zabezpečení SMTP a POP3 komunikace protokolem TLS.

Při použití protokolu TLS se nejprve naváže nešifrované spojení a poté se klient se serverem dohodnou na přepnutí do zabezpečeného režimu (šifrované spojení). Pokud klient nebo server

protokol TLS nepodporuje, pak k přepnutí do zabezpečeného režimu nedojde a komunikace probíhá nešifrovaným spojením.

Je-li spojení šifrováno, pak jej firewall nemůže analyzovat a provádět antivirovou kontrolu přenášených zpráv. Správce *WinRoute* proto může nastavit jednu z následujících možností:

- Povolit zabezpečení protokolem TLS. Tato volba je vhodná v případech, kdy je ochrana spojení proti odposlechu důležitější než antivirová kontrola zpráv.

  Tip

  V tomto případě je doporučeno nainstalovat na jednotlivé počítače uživatelů (pracovní stanice) antivirový program, který bude provádět antivirovou kontrolu pošty lokálně.

- Zakázat zabezpečení TLS. Firewall bude blokovat přepnutí spojení do zabezpečeného režimu. Klient se bude domnívat, že server protokol TLS nepodporuje, a zprávy budou přenášeny nezabezpečeným spojením. Firewall pak bude moci provádět antivirovou kontrolu všech přenášených zpráv.

Pole *Nemůže-li být příloha zkontrolována* obsahuje volby pro případ, že ve zprávě bude nalezena jedna nebo více příloh, které nelze zkontrolovat antivirovým programem (např. archiv chráněný heslem, poškozený soubor apod.):

- *Zakázat doručení této přílohy* — *WinRoute* se zachová stejně jako v případě detekce viru (včetně výše popsaných akcí).
- *Povolit doručení této přílohy* — *WinRoute* bude předpokládat, že šifrované či poškozené přílohy neobsahují viry.
  Tato volba obecně není bezpečná, ale lze ji využít např. v případě, kdy uživatelé odesílají či přijímají velké množství šifrovaných souborů (typicky archivů chráněných heslem) a na pracovních stanicích je nainstalován antivirový program.

13.5 Kontrola souborů přenášených Clientless SSL-VPN (Windows)

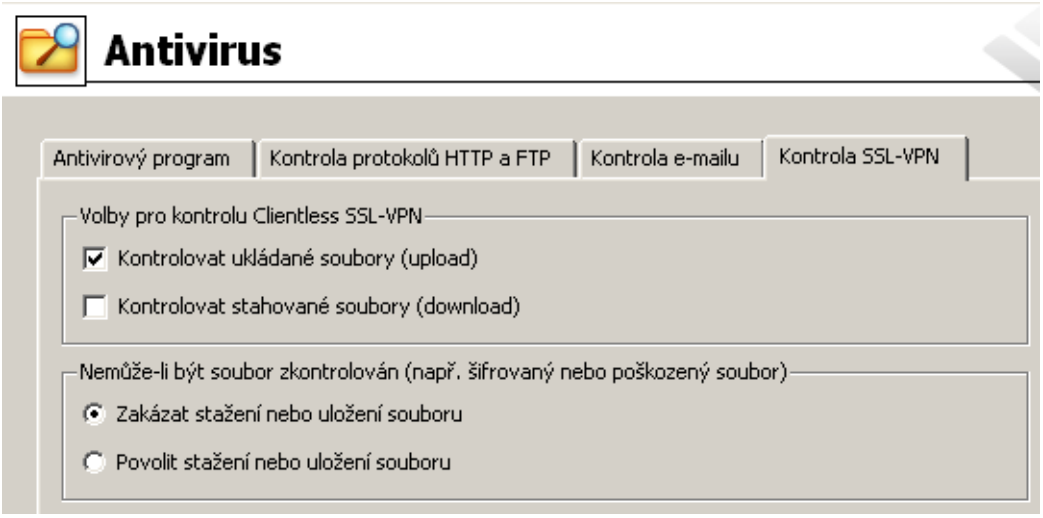
Je-li *WinRoute* nainstalován na systému *Windows*, pak se antivirová kontrola rovněž provádí při přenosu souborů mezi lokální sítí a vzdáleným klientem prostřednictvím rozhraní *Clientless SSL-VPN* (viz kapitola 24). Záložka *Kontrola SSL-VPN* umožňuje nastavit upřesňující parametry pro kontrolu souborů přenášených tímto rozhraním. Při správě *Kerio WinRoute Firewall Software Appliance / VMware Virtual Appliance* není záložka *Kontrola SSL-VPN* k dispozici.

Kontrola jednotlivých směrů přenosu

V horní části záložky *Kontrola SSL-VPN* lze nastavit, pro který směr přenosu se má antivirová kontrola provádět. Ve výchozí konfiguraci se z důvodu rychlosti kontrolují pouze soubory ukládané ze vzdáleného klienta na počítač v lokální síti (lokální síť je považována za důvěryhodnou).

Akce při selhání antivirové kontroly

Tyto volby specifikují akci, která bude provedena, pokud nemůže antivirový program určitý soubor z nějakého důvodu zkontrolovat (typicky šifrovaný archiv nebo poškozený soubor). Ve výchozí konfiguraci je z bezpečnostních důvodů přenos takových souborů zakázán.



Obrázek 13.10 Parametry antivirové kontroly souborů přenášených rozhraním Clientless SSL-VPN

Kapitola 14

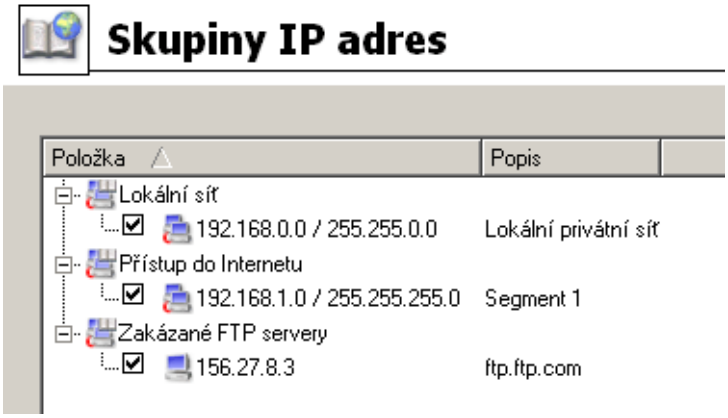
Definice

14.1 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*.



Obrázek 14.1 Skupiny IP adres ve WinRoute

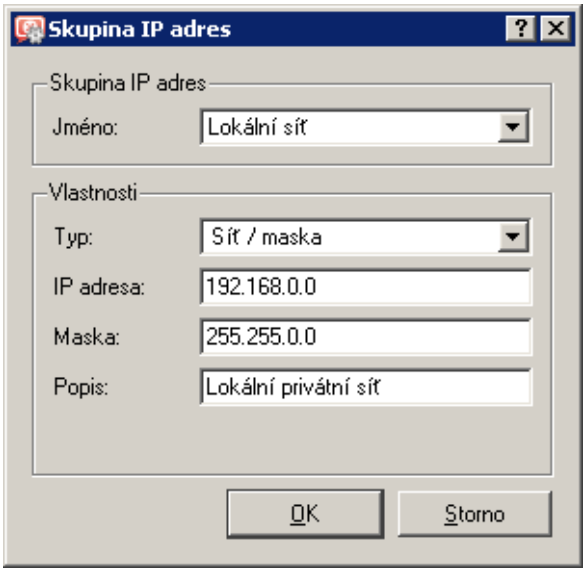
Tlačítkem *Přidat* lze přidat novou skupinu (nebo položku do existující skupiny), tlačítkem *Změnit* upravit a tlačítkem *Odebrat* smazat vybranou skupinu či položku.

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:

- *Počítač* (IP adresa nebo DNS jméno konkrétního počítače),
- *Síť / maska* (subsíť s příslušnou maskou),
- *Rozsah IP adres* (interval zadaný počáteční a koncovou adresou včetně),



Obrázek 14.2 Definice položky skupiny IP adres a/nebo nové skupiny

- *Skupina adres* (jiná skupina IP adres — skupiny adres lze do sebe vnořovat),
- *Firewall* (speciální skupina zahrnující všechny IP adresy všech rozhraní firewallu, viz též kapitola 7.3).

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

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

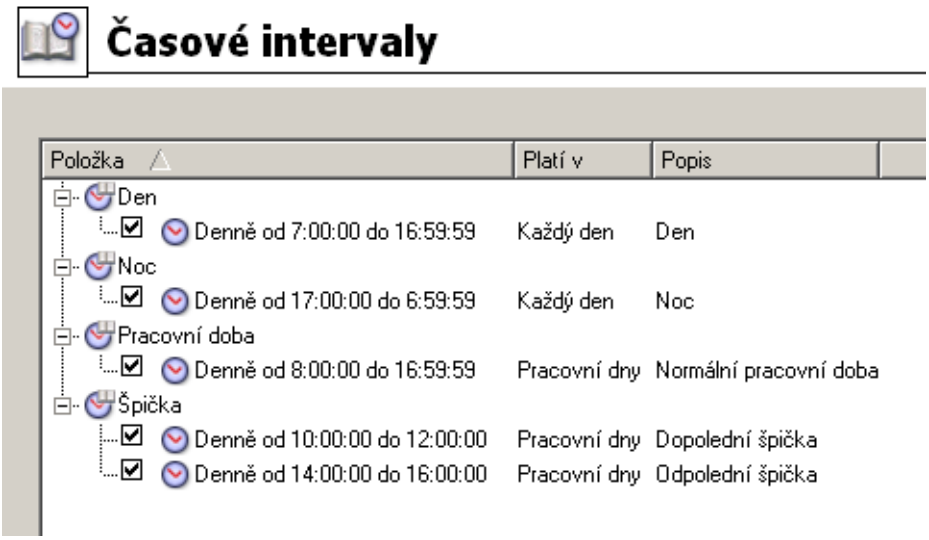
Poznámka: Každá skupina IP adres musí obsahovat alespoň jednu položku. Odebráním poslední položky skupina zanikne.

14.2 Časové intervaly

Časové intervaly jsou ve *WinRoute* úzce propojeny s komunikačními pravidly (viz kapitola 7). 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 kapitola 5.

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



Obrázek 14.3 Časové intervaly ve WinRoute

Typy časových intervalů

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

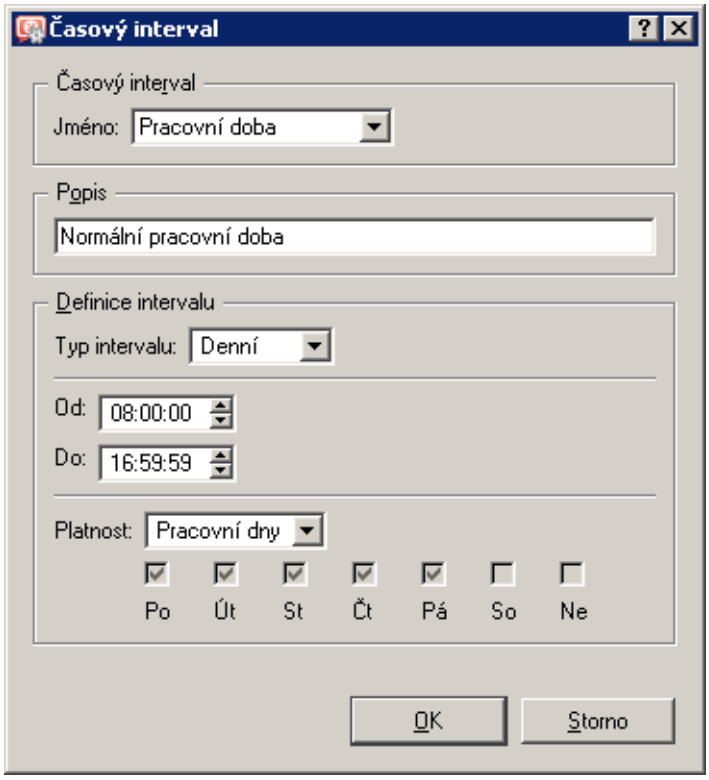
Časový interval lze vytvořit, upravit nebo smazat v sekci *Konfigurace* → *Definice* → *Časové intervaly*.

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



Obrázek 14.4 Definice položky časového intervalu a/nebo nového intervalu

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).

Poznámka:

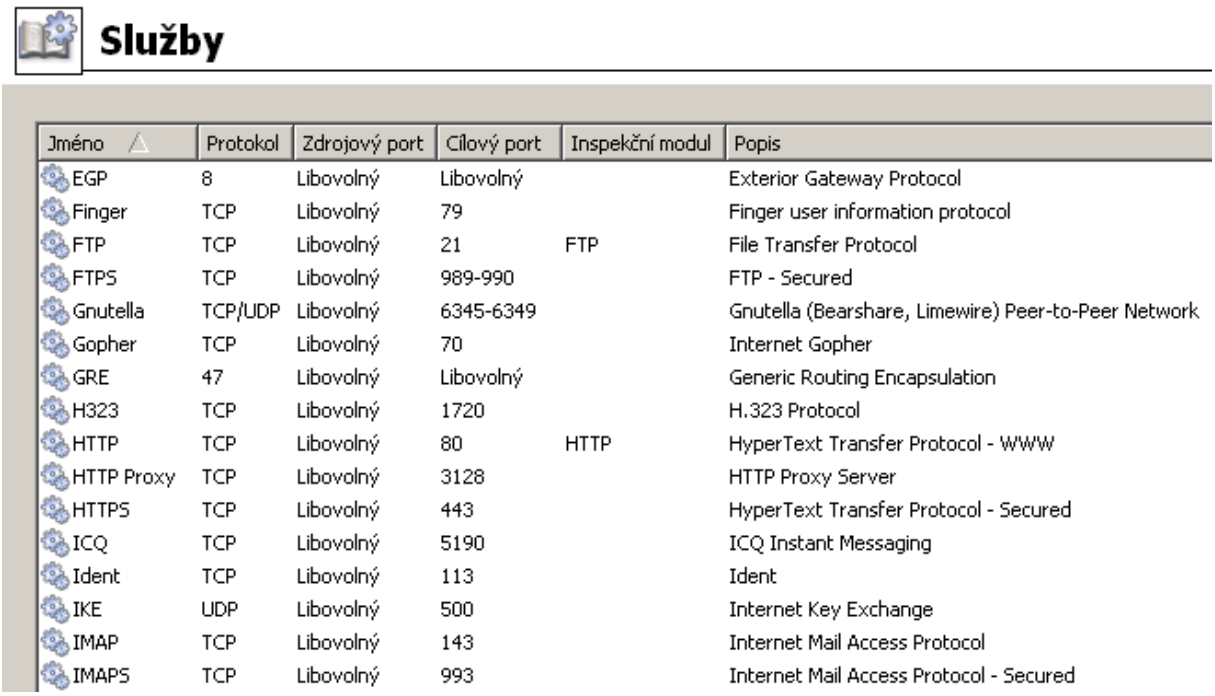
1. Každý časový interval musí obsahovat alespoň jednu položku. Odebráním poslední položky časový interval zanikne.

2. Vytvořené časové intervaly nelze do sebe vnořovat.

14.3 Služby

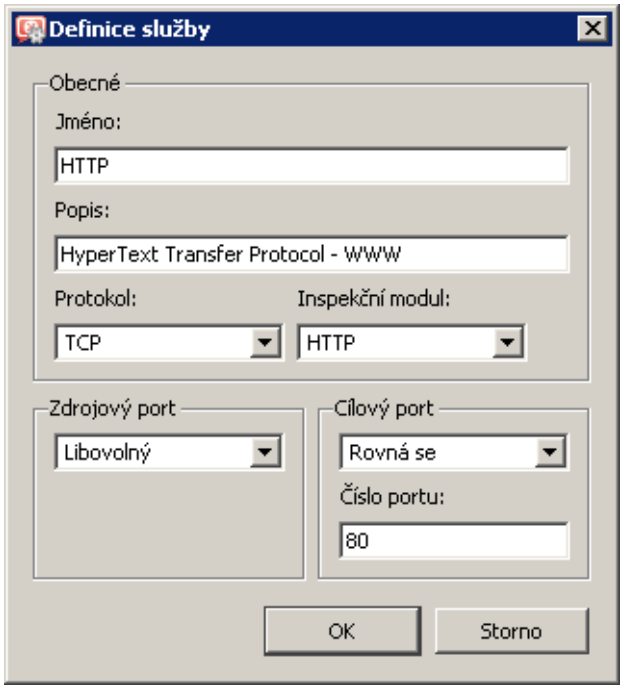
ve *WinRoute* usnadňují definici komunikačních pravidel (povolení či zakázání přístupu z lokální sítě do Internetu nebo naopak zpřístupnění lokálního serveru z Internetu). Zjednodušeně lze říci, že služba je definována komunikačním protokolem a číslem portu, na kterém je přístupná (např. služba *HTTP* 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.).



Obrázek 14.5 Síťové služby ve WinRoute

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



Obrázek 14.6 Definice síťové služby

Jméno

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

Popis

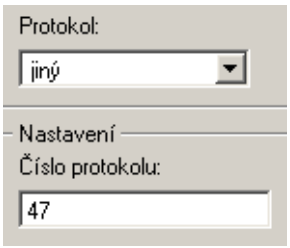
Textový popis definované služby. Doporučujeme popisovat důsledně význam každé definice, zejména pokud se jedná o nestandardní služby — ušetříte si mnoho času a námahy při pozdějším odhalování chyb či předávání *WinRoute* jinému správci.

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).



Obrázek 14.7 Nastavení protokolu v definici služby

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.

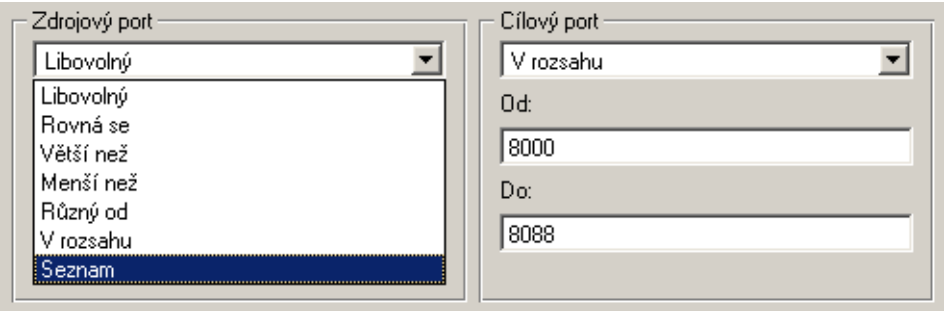
Zdrojový a cílový port

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 7.3.

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)



Obrázek 14.8 Nastavení zdrojového a cílového portu v definici služby

- *Seznam* — seznam portů oddělených čárkami (např.: `80,8000,8080`)

Inspekční moduly

WinRoute obsahuje speciální moduly, které sledují komunikaci daným aplikačním protokolem (např. HTTP, FTP apod.). Tuto komunikaci pak mohou určitým způsobem modifikovat (filtrovat) nebo přizpůsobit chování firewallu danému protokolu. Činnost inspekčních modulů bude objasněna 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 příslušná komunikace je povolena. Každý inspekční modul obsluhuje protokol, pro který je určen, a službu, v jejíž definici je použit. Ve výchozí konfiguraci *WinRoute* jsou všechny dostupné inspekční moduly použity v definici příslušných služeb (a budou tedy automaticky aplikovány na odpovídající komunikaci), s výjimkou inspekčních modulů protokolů pro hlasové služby *SIP* a *H.323* (*SIP* a *H.323* jsou komplexní protokoly a inspekční moduly nemusí v některých konfiguracích fungovat správně).

Chceme-li explicitně aplikovat inspekční modul na jinou komunikaci, musíme buď definovat novou službu s použitím tohoto modulu nebo nastavit inspekční modul přímo v příslušném komunikačním pravidle.

Příklad

Chceme provádět inspekci protokolu HTTP na nestandardním portu 8080. Definujeme novou službu: protokol TCP, port 8080, inspekční modul HTTP. Tím je zajištěno, že na komunikaci protokolem *TCP* na portu 8080 procházející přes *WinRoute* bude automaticky aplikován inspekční modul protokolu *HTTP*.

Poznámka:

1. Inspekční moduly obecně nelze použít pro zabezpečenou komunikaci (SSL/TLS). V tomto případě *WinRoute* „vidí“ pouze binární data — komunikaci nelze dešifrovat.

2. V některých případech nemusí být aplikace inspekčního modulu na určitou komunikaci žádoucí. Nastane-li tato situace, je možné příslušný inspekční modul „vyřadit“. Podrobnosti naleznete v kapitole 7.7.

14.4 Skupiny URL

Skupiny URL slouží ke snadné a přehledné definici pravidel pro HTTP (viz kapitola 12.2). 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 je rovněž možné do sebe vnořovat.

Skupiny URL se definují v sekci *Konfigurace* → *Definice* → *Skupiny URL*.

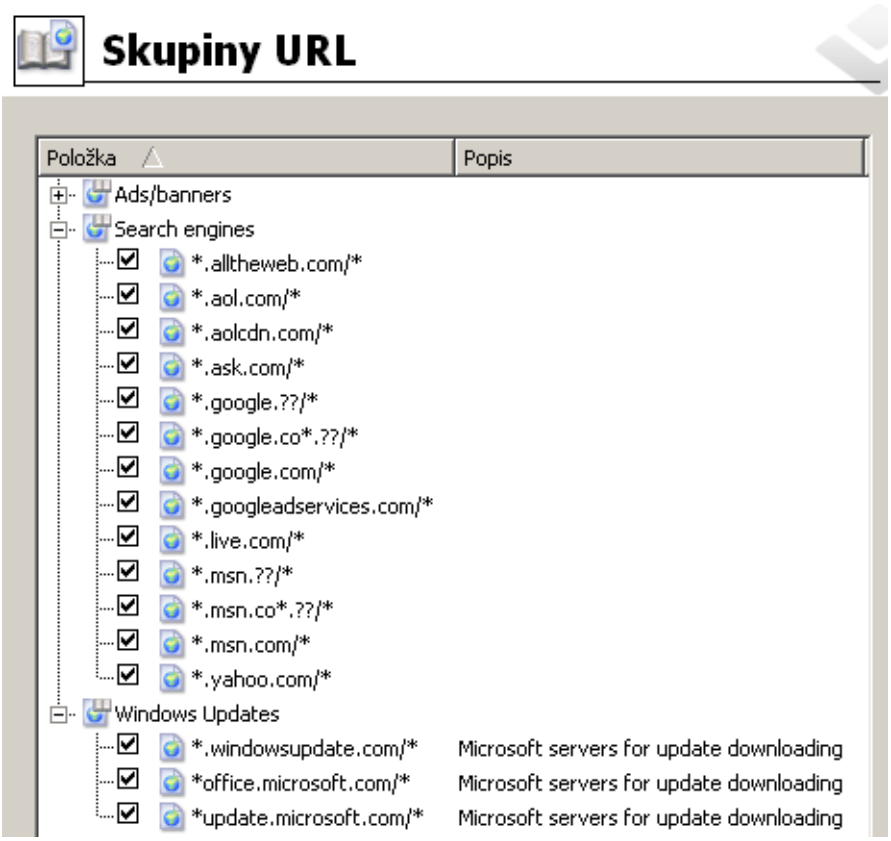
Výchozí instalace *WinRoute* obsahuje tyto předdefinované skupiny URL:

- *Ads/Banners* — typická URL stránek zobrazujících reklamy, reklamních pruhů na stránkách apod.
- *Search engines* — nejpoužívanější internetové vyhledávače.
- *Windows Updates* — URL stránek, ze kterých se stahují automatické aktualizace systému Windows.

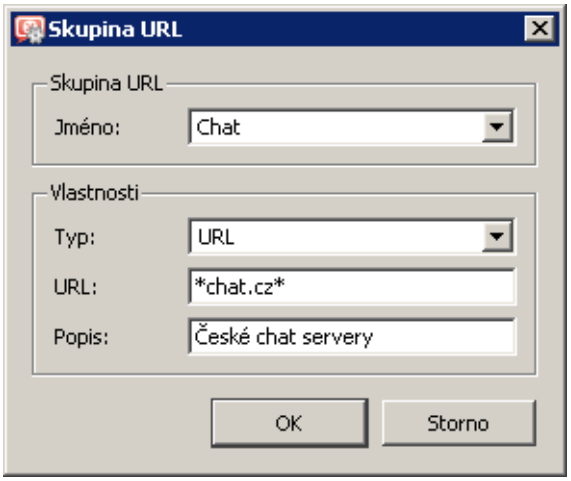
Tyto skupiny URL jsou použity v předdefinovaných pravidlech pro URL (viz kapitola 12.2). Správce *WinRoute* samozřejmě může předdefinované skupiny použít ve vlastních pravidlech, případně je upravit dle svého uvážení.

Zaškrtávací pole vedle každé položky skupiny slouží k její aktivaci a deaktivaci. Takto lze položku dočasně vyřadit ze skupiny bez nutnosti ji odebírat a poté znovu přidávat.

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



Obrázek 14.9 Skupiny URL



Obrázek 14.10 Definice položky skupiny URL a/nebo nové skupiny

Jméno

Jméno skupiny, do které má být přidána nová položka. V poli *Jméno* je možné:

- vybrat některou z existujících skupin,
- zadat jméno nové (dosud neexistující) skupiny — tím dojde k vytvoření nové skupiny, do které bude nová položka zařazena.

Typ

Typ přidávané položky — URL nebo skupina URL (skupiny lze do sebe vnořovat).

URL / Skupina URL

URL nebo skupina URL, která má být do skupiny přidána (v závislosti na zvoleném typu položky).

URL může být specifikováno 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 přidávané položky skupiny (pro snazší orientaci).

Kapitola 15

Uživatelské účty a skupiny

Uživatelské účty ve *WinRoute* slouží pro lepší řízení přístupu uživatelů z lokální sítě ke službám v Internetu. Uživatelský účet může být použit také pro přístup ke správě *WinRoute* pomocí programu *Administration Console* nebo rozhraní *Web Administration*.

WinRoute podporuje několik různých způsobů uložení uživatelských účtů a skupin v kombinaci s různými způsoby ověřování uživatelů:

Interní databáze uživatelů

Uživatelské účty a skupiny uživatelů jsou uloženy přímo ve *WinRoute*, a to včetně hesla. Při ověřování uživatele se zadané uživatelské jméno zkontroluje s údaji v interní databázi.

Tento způsob uložení účtů a ověřování uživatelů je vhodný především pro sítě bez domény a pro speciální administrátorské účty (i při výpadku sítě se lze přihlásit a ověřit lokálně).

V sítích s doménou (*Windows NT* nebo *Active Directory*) však představují lokální účty ve *WinRoute* značné zvýšení administrativních nároků — účty a hesla je nutné udržovat na dvou místech (doména a *WinRoute*).

Interní databáze uživatelů s ověřováním v doméně

Uživatelské účty jsou uloženy ve *WinRoute*, ale uživatelé se ověřují v doméně *Windows NT* nebo *Active Directory* (tzn. v uživatelském účtu ve *WinRoute* není uloženo heslo). Uživatelské jméno ve *WinRoute* a v doméně musí být totožné.

Z hlediska administrativy je tento způsob uložení účtů a ověřování uživatelů podstatně méně náročný — pokud si např. uživatel chce změnit heslo, stačí jej změnit v doméně a tato změna se automaticky promítne také do účtu ve *WinRoute*. Uživatelské účty ve *WinRoute* navíc není nutné vytvářet ručně, lze je importovat z příslušné domény.

Automatický import účtů z Active Directory

Při použití *Active Directory* (*Windows 2000 Server* nebo *Windows Server 2003/2008*) lze nastavit tzv. automatický import uživatelských účtů. Ve *WinRoute* není třeba definovat ani importovat žádné uživatelské účty, stačí vytvořit šablonu, podle které budou uživateli nastaveny specifické parametry pro *WinRoute* (např. přístupová práva, pravidla pro obsah WWW stránek, kvóty objemu přenesených dat apod.). Uživatelský účet bude do *WinRoute* automaticky importován po prvním úspěšném přihlášení uživatele. Parametry nastavené šablonou lze v případě potřeby u konkrétních účtů změnit.

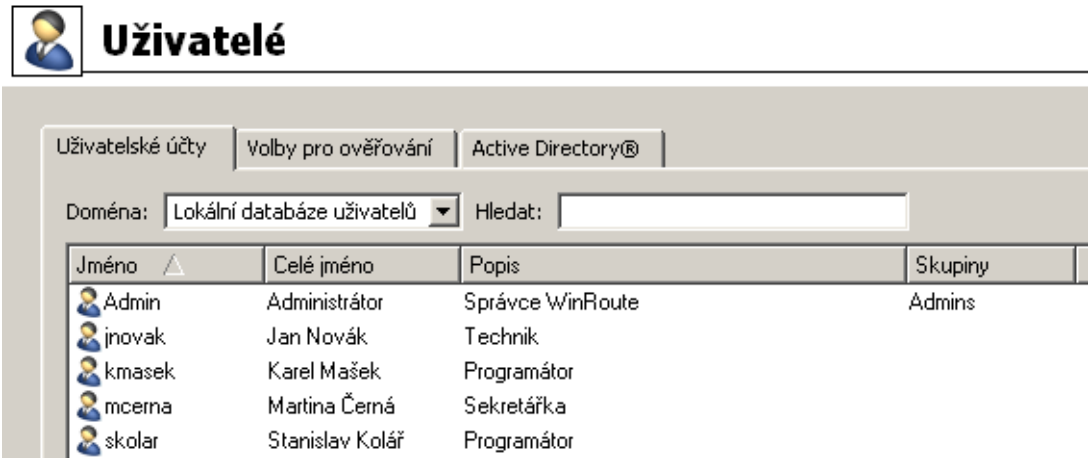
Poznámka: Tento způsob spolupráce s *Active Directory* je určen zejména pro zachování zpětné kompatibility se staršími verzemi *WinRoute*. V případě „čisté“ instalace *WinRoute* doporučujeme použít transparentní spolupráci s *Active Directory*.

Transparentní spolupráce s Active Directory (mapování domény)
: *WinRoute* může používat přímo účty a skupiny uložené v *Active Directory* — neprovádí se žádný import do lokální databáze. Specifické parametry pro *WinRoute* jsou dodány šablonou účtu, případně je lze nastavit individuálně (stejně jako v předchozím případě). Tento způsob je administrativně nejméně náročný (veškerá správa uživatelských účtů a skupin probíhá pouze v *Active Directory*) a jako jediný umožňuje použití účtů z více různých *Active Directory* domén.

Poznámka: V případě ověřování uživatelů v doméně (tj. všechny popsané způsoby s výjimkou prvního) je doporučeno vytvořit ve *WinRoute* alespoň jeden lokální účet s přístupem ke správě pro čtení i zápis ověřovaný v interní databázi uživatelů (resp. ponechat originální účet `Admin`). Tento účet umožní připojení ke správě *WinRoute* i při výpadku sítě nebo doménového serveru.

15.1 Zobrazení a definice uživatelských účtů

K definici lokálních uživatelských účtů, importu účtů do lokální databáze a nastavení parametrů účtů mapovaných z domény slouží sekce *Uživatelé a skupiny* → *Uživatelé*, záložka *Uživatelské účty*.



Obrázek 15.1 Uživatelské účty ve WinRoute

Doména
: Volba *Doména* umožňuje vybrat doménu, pro kterou budeme definovat uživatelské účty a další parametry. V této položce lze zvolit některou z mapovaných *Active Directory* domén (viz kapitola 15.4) nebo lokální (interní) databázi uživatelů.

Vyhledávání
: Funkce *Hledat* umožňuje zadat filtr pro zobrazení uživatelských účtů.
Vyhledávání je interaktivní — s každým zadaným (resp. smazaným) znakem se zobrazí všechny účty obsahující zadaný řetězec znaků v položce *Jméno*, *Celé jméno* nebo *Popis*. Kliknutím na ikonu vedle pole pro zadání hledaného řetězce se filtr zruší a zobrazí se všechny uživatelské účty ve vybrané doméně (pokud je pole *Hledat* prázdné, ikona pro zrušení filtru je skryta).

Vyhledávání je užitečné zejména při velkém počtu uživatelů, kdy by nalezení požadovaného účtu klasickou cestou bylo značně zdlouhavé.

Zobrazení / skrytí zakázaných účtů
Některé uživatelské účty mohou být ve *WinRoute* zakázány (zablokovány). Volba *Skrýt zakázané uživatelské účty* umožňuje zobrazit pouze aktivní (povolené) účty, což zpřehledňuje seznam účtů.

Šablona účtu
Parametry, které jsou pro všechny účty (resp. většinu účtů) shodné, lze definovat hromadně tzv. šablonou. Použití šablony výrazně zjednodušuje správu uživatelských účtů — společné parametry stačí nastavit pouze jednou v definici šablony. U vybraných účtů (např. administrátorských) je možné nastavit všechny parametry individuálně bez použití šablony.
Šablona účtu je specifická pro vybranou doménu (resp. lokální databázi uživatelů). Šablona obsahuje nastavení uživatelských práv, kvót objemu přenesených dat a pravidel pro komponenty WWW stránek (podrobný popis jednotlivých parametrů viz kapitola 15.2).

Lokální uživatelské účty

Volbou *Lokální databáze uživatelů* v položce *Doména* se zobrazí lokální uživatelské účty ve *WinRoute* (všechny informace o těchto účtech jsou uloženy v konfigurační databázi *WinRoute*). Pro účty v lokání databázi jsou k dispozici následující volby:

Přidání, změna a odebrání účtu
Pomocí tlačítek *Přidat*, *Změnit* a *Odebrat* lze vytvářet, upravovat a rušit lokální uživatelské účty dle potřeby (podrobnosti viz kapitola 15.2). Po označení dvou nebo více účtů (s pomocí kláves `Ctrl` a `Shift`) lze provést tzv. hromadnou změnu účtů, tj. nastavení určitých parametrů všem označeným účtům.

Import účtů z domény
Do lokální databáze uživatelů lze importovat účty z domény *Windows NT* nebo *Active Directory*. Jedná se de facto o automatické vytvoření lokálních účtů odpovídajících vybraným doménovým účtům s ověřováním v příslušné doméně. Podrobné informace o importu uživatelských účtů naleznete v kapitole 15.3.
Import účtů je vhodné použít v případě domény *Windows NT*. Při použití *Active Directory* domény je výhodnější využít transparentní spolupráci s *Active Directory* (mapování domény — viz kapitola 15.4).

Mapované účty z Active Directory domény

Výběrem některé z mapovaných *Active Directory* domén v položce *Doména* se zobrazí seznam uživatelských účtů v této doméně.

Změna účtu
U mapovaných účtů lze nastavit parametry specifické pro *WinRoute* (podrobnosti viz kapitola 15.2). Tato nastavení budou uložena do konfigurační databáze *WinRoute*. Údaje

uložené v *Active Directory* (uživatelské jméno, celé jméno, e-mailovou adresu) a způsob ověřování uživatele nelze změnit.
Poznámka: Po označení dvou nebo více účtů (s pomocí kláves `Ctrl` a `Shift`) lze provést tzv. hromadnou změnu účtů, tj. nastavení určitých parametrů všem označeným účtům.

V mapovaných *Active Directory* doménách nelze vytvářet ani rušit uživatelské účty. Tyto akce musí být prováděny přímo v databázi *Active Directory* na příslušném doménovém serveru. Rovněž není možný import uživatelských účtů — taková akce nemá v případě mapované domény smysl.

15.2 Lokální uživatelské účty

Lokální účty jsou účty vytvořené ve *WinRoute* nebo importované z domény. Tyto účty jsou uloženy v konfigurační databázi *WinRoute* (viz kapitola 25.2). Tyto účty lze využít zejména v prostředích bez domény a pro speciální účely (typicky pro správu firewallu).

Nezávisle na tom, jak byl konkrétní účet vytvořen, může být každý uživatel ověřován v interní databázi *WinRoute*, v *Active Directory* nebo v doméně *Windows NT*.

Základní administrátorský účet `Admin` 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 ke všem uživatelským účtům by měla být důsledně uchovávána v tajnosti, aby nemohlo dojít k jejich zneužití neoprávněnou osobou.

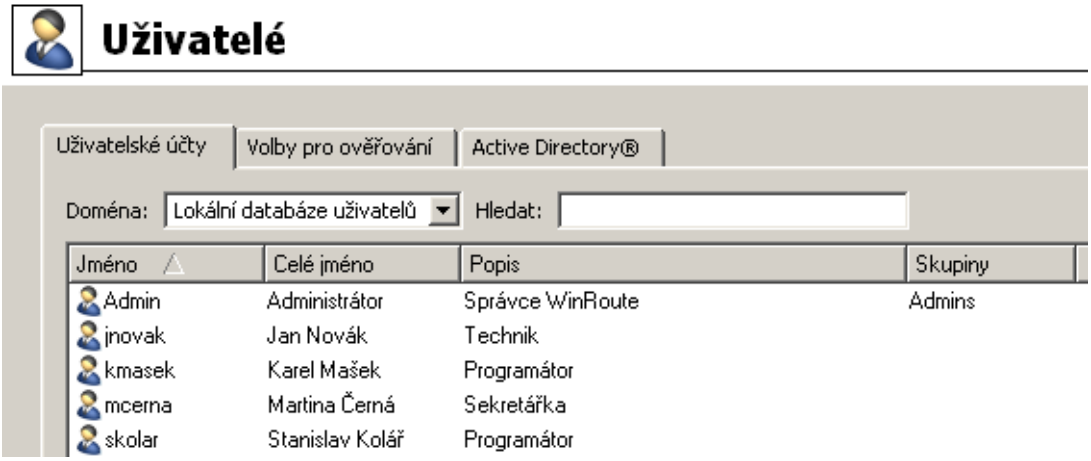
2. Odstraníte-li poslední účet s plnými právy ke správě a odhlásíte se ze správy *WinRoute*, nebude již možné se ke správě znovu přihlásit. V takovém případě bude při dalším startu *WinRoute Firewall Engine* automaticky vytvořen lokální uživatelský účet `Admin` s prázdný heslem.

3. V případě zapomenutí administrátorského hesla kontaktujte technickou podporu firmy *Kerio Technologies* (viz kapitola 26).

Vytvoření lokálního uživatelského účtu

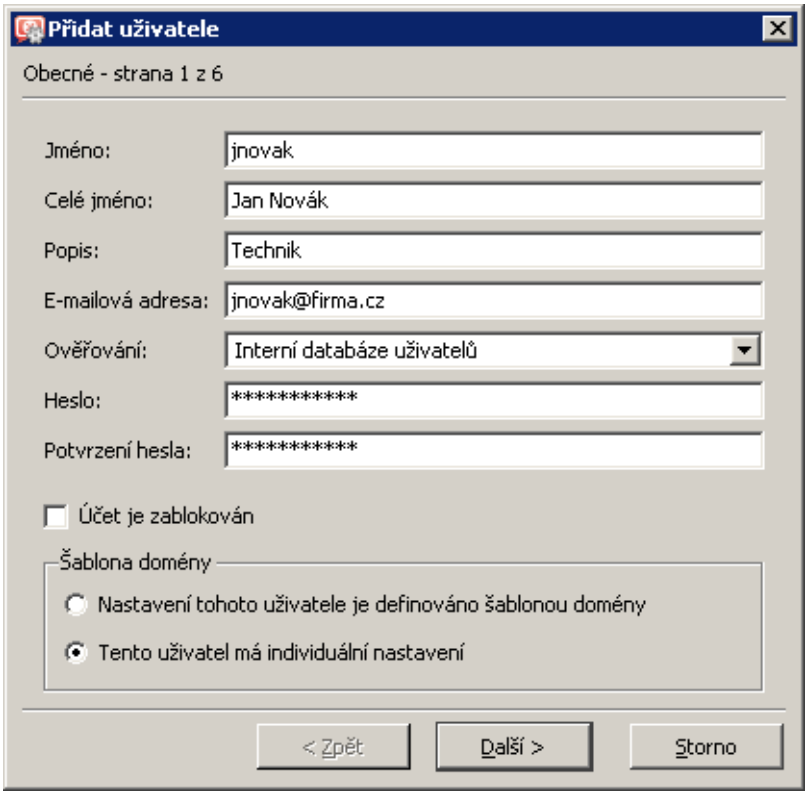
Přepneme se do sekce *Uživatelé a skupiny* → *Uživatelé*, záložka *Uživatelské účty*. V položce *Doména* zvolíme *Lokální databáze uživatelů*.

Stisknutím tlačítka *Přidat* se zobrazí průvodce vytvořením nového uživatelského účtu.



Obrázek 15.2 Lokální uživatelské účty ve WinRoute

Krok 1 — základní údaje



Obrázek 15.3 Vytvoření uživatelského účtu — základní parametry

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 do webových rozhraní firewallu.

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.

E-mailová adresa

E-mailová adresa uživatele pro zasílání výstrah (viz kapitola 19.4) a dalších zpráv (např. varování o překročení limitu objemu přenesených dat). Pro efektivní využití všech funkcí *WinRoute* je třeba každému uživateli nastavit platnou e-mailovou adresu.

Poznámka: Pro zasílání e-mailových zpráv uživatelům musí být ve *WinRoute* nastaven server odchozí pošty. Podrobnosti naleznete v kapitole 18.3.

Ověřování

Způsob ověřování uživatele (viz dále).

Účet je zablokován

Dočasné zrušení („vypnutí“) účtu bez nutnosti jej odstraňovat.

Poznámka: V průvodci pro vytvoření nového účtu lze tuto volbu využít např. pro vytvoření účtu uživateli, který jej nebude používat ihned (nový zaměstnanec, který dosud nenastoupil na své místo apod.).

Šablona domény

Volba způsobu, jakým budou nastaveny parametry tohoto uživatelského účtu (přístupová práva, kvóty objemu přenesených dat a pravidla pro obsah WWW stránek). Tyto parametry mohou být definovány šablonou příslušné domény (viz kapitola 15.1) nebo nastaveny individuálně pro konkrétní účet.

Šablonu je vhodné použít pro „standardní“ účty v dané doméně (např. účty běžných uživatelů). Definice účtů se tím výrazně zjednoduší — průvodce vytvořením účtu bude zkrácen o 3 kroky.

Individuální nastavení je vhodné zejména pro účty se speciálními právy (např. účty pro správu *WinRoute*). Těchto účtů bývá zpravidla malý počet, a proto jejich vytvoření a individuální nastavení parametrů není příliš náročné.

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 manuál *Kerio WinRoute Firewall — Příručka uživatele*).

Upozornění

1. 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 do WWW rozhraní.
2. Při tomto způsobu ověřování uživatelů nelze použít automatické ověřování uživatelů metodou NTLM (viz kapitola 25.3). Tyto účty rovněž nelze použít pro přístup do rozhraní *Clientless SSL-VPN* (viz kapitola 24).

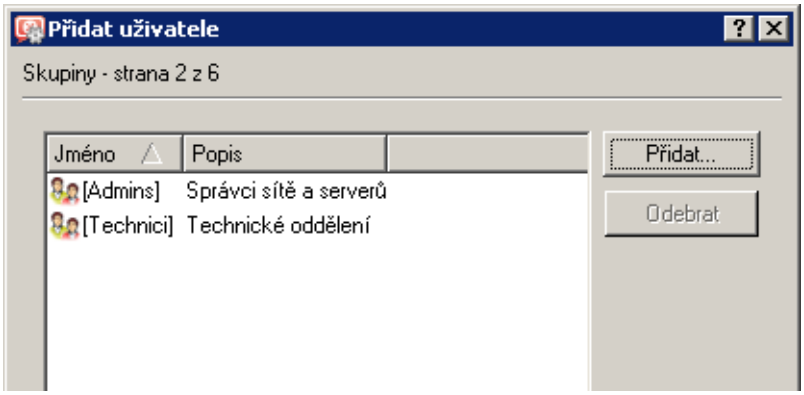
NT doména / Kerberos 5

Uživatel bude ověřován v doméně *Windows NT* (*Windows NT 4.0*) nebo v *Active Directory* (*Windows 2000/2003/2008*).

Parametry pro ověřování uživatelů v doméně *Windows NT* a/nebo *Active Directory* je třeba nastavit v záložce *Active Directory / NT doména* sekce *Uživatelé*. Je-li nastaveno ověřování v *Active Directory* i v doméně *Windows NT*, pak má *Active Directory* přednost.

Poznámka: Nebude-li povoleno ověřování ani v Active Directory ani v NT doméně, pak budou uživatelské účty s tímto typem ověřování neaktivní. Podrobnosti viz kapitola 15.3.

Krok 2 — skupiny



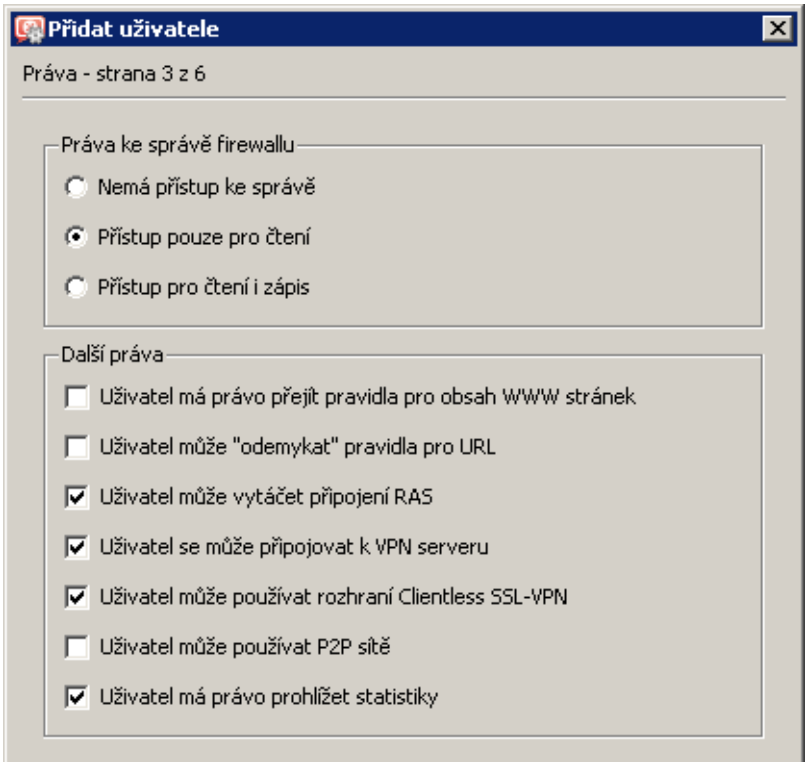
Obrázek 15.4 Vytvoření uživatelského účtu — skupiny

V tomto dialogu lze (tlačítky *Přidat* a *Odebrat*) přidat nebo odebrat skupiny, do kterých má být uživatel zařazen (skupiny se definují v sekci *Uživatelé a skupiny* → *Skupiny* — viz kapitola 15.5). 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 lze označit více skupin najednou přidržením klávesy *Ctrl* nebo *Shift*.

Krok 3 — přístupová práva



Obrázek 15.5 Vytvoření uživatelského účtu — uživatelská práva

Každý uživatel musí mít nastavenu jednu ze tří úrovní přístupových práv.

Nemá přístup 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 nastavení a záznamy, 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.

Doplňková práva:

Uživatel má právo přejít pravidla...
: Tato volba umožňuje uživateli měnit osobní nastavení filtrování obsahu WWW stránek nezávisle na nastavení (podrobnosti viz *Krok 5*).

Uživatel může „odemykat“ pravidla pro URL
: Po zaškrtnutí volby je uživateli povoleno jednorázově obejít zákaz přístupu na blokované WWW stránky — na stránce s informací o zákazu se tomuto uživateli zobrazí tlačítko *Odemknout*. Odemknutí musí být zároveň povoleno v příslušném pravidle pro URL (podrobnosti viz kapitola 12.2).

Uživatel může vytáčet připojení RAS
Pokud je připojení k Internetu realizováno vytáčenými linkami, uživatel bude moci tyto linky vytáčet a zavěšovat prostřednictvím WWW rozhraní firewallu (viz kapitola 11).

Uživatel se může připojovat k VPN serveru
Uživatel má právo připojit se k VPN serveru ve *WinRoute* (aplikací *Kerio VPN Client*). Podrobné informace naleznete v kapitole 23.

Uživatel může používat rozhraní Clientless SSL-VPN
Tento uživatel bude moci přistupovat ke sdíleným souborů a složkám v lokální síti prostřednictvím webového rozhraní *Clientless SSL-VPN*.
Rozhraní *Clientless SSL-VPN* a příslušné uživatelské právo je k dispozici pouze ve *WinRoute* pro systém *Windows*. Podrobnosti viz kapitola 24.

Uživatel může používat P2P sítě
Na tohoto uživatele nebude aplikováno blokování komunikace při detekci *P2P* (*Peer-to-Peer*) sítí. Podrobnosti viz kapitola 17.1.

Uživatel má právo prohlížet statistiky
Tento uživatel bude mít přístup ke statistikám firewallu zobrazovaným ve WWW rozhraní (viz kapitola 11).

Tip

Přístupová práva mohou být nastavena šablonou uživatelského účtu.

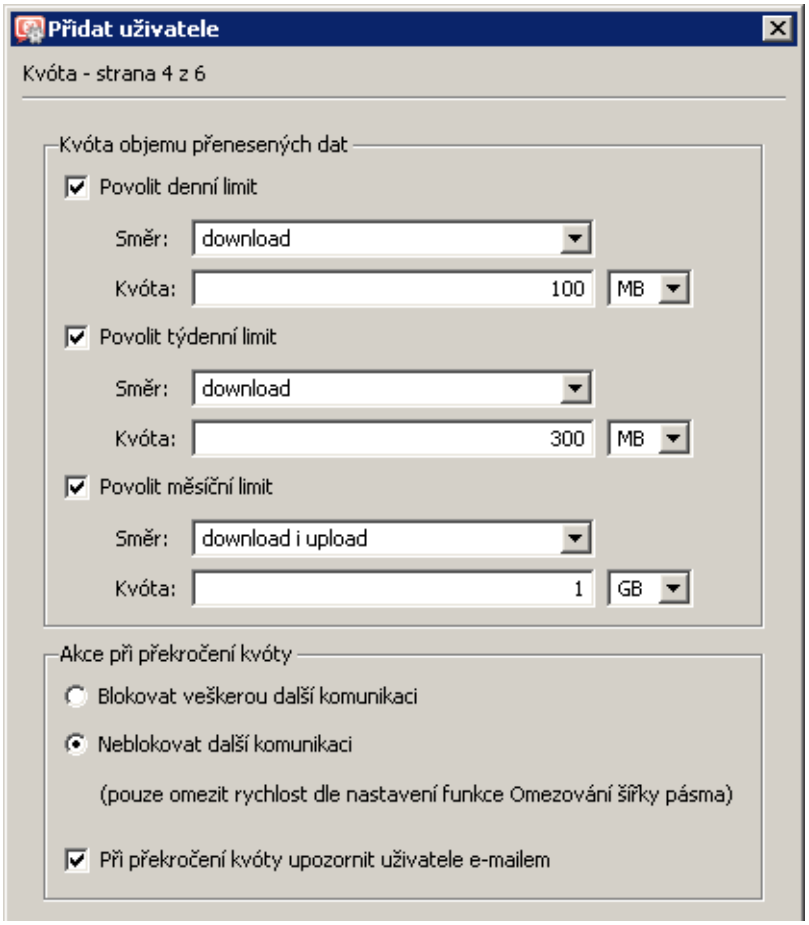
Krok 4 — kvóta objemu přenesených dat

V tomto kroku průvodce lze nastavit denní a měsíční limit objemu dat přenesených daným uživatelem přes firewall a akce, které budou provedeny.

Kvóta objemu přenesených dat
Nastavení denního, týdenního a měsíčního limitu objemu přenesených dat pro daného uživatele.
V položce *Směr* lze vybrat, jaký směr přenosu dat bude sledován (*download* — přijímaná data, *upload* — vysílaná data, *download i upload* — součet v obou směrech).
Do položky *Kvóta* je třeba zadat požadovaný limit ve vybraných jednotkách (megabyty nebo gigabyty).

Akce při překročení kvóty
Nastavení akcí, které mají být provedeny při překročení některého limitu:

- *Blokovat veškerou další komunikaci* — uživatel bude moci dále komunikovat v rámci již otevřených spojení, nebude však moci navázat žádná nová spojení (tzn. např. připojit se na nový server, stáhnout další soubor v FTP relaci apod.).
- *Neblokovat další komunikaci (pouze omezit rychlost...)* — uživateli bude omezena rychlost internetové komunikace (tzv. šířka pásma). Nic nebude blokováno, ale uživatel zaznamená výrazné zpomalení internetové komunikace (což by jej mělo přimět k omezení jeho aktivit). Podrobné informace viz kapitola 9.



Obrázek 15.6 Vytvoření uživatelského účtu — kvóta objemu dat

Zapnutím volby *Při překročení kvóty upozornit uživatele e-mailem* bude uživateli zasláno e-mailem varování při překročení některého z nastavených limitů. Podmínkou je, aby měl uživatel nastavenu platnou e-mailovou adresu (viz *Krok 1* tohoto průvodce). Ve *WinRoute* musí být nastaven server odchozí pošty (viz kapitola 18.3).
Má-li být při překročení kvóty některým uživatelem varován také správce *WinRoute*, můžeme nastavit příslušnou výstrahu v sekci *Konfigurace* → *Statistiky a záznamy*. Podrobnosti naleznete v kapitole 19.4.
Poznámka:

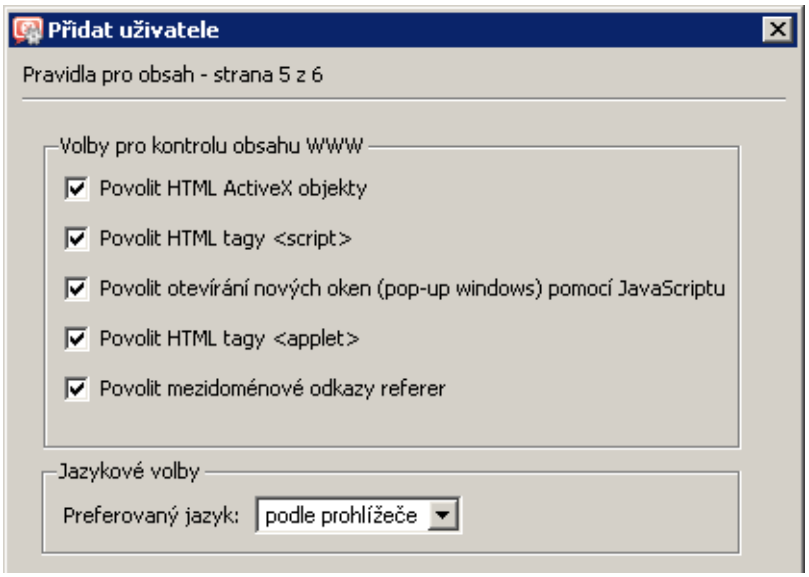
1. Je-li při překročení limitu zablokována komunikace, platí omezení až do konce příslušného období (tj. dne nebo měsíce). Zrušení omezení před skončením tohoto období je možné:
    - (dočasným) vypnutím příslušného limitu, zvýšením tohoto limitu nebo změnou akce na *Neblokovat další komunikaci*,
    - smazáním čítačů objemu přenesených dat příslušného uživatele (viz kapitola 20.1).
2. Akce při překročení kvóty se neprovádějí, pokud je uživatel přihlášen přímo na firewallu. V takovém případě by totiž mohlo dojít k blokování komunikace firewallu a

tím i všech uživatelů v lokální síti. Přenesená data se však do kvóty započítávají!

Tip

Kvóty objemu přenesených dat a odpovídající akce mohou být nastaveny šablonou uživatelského účtu.

Krok 5 — pravidla pro obsah WWW stránek a preferovaný jazyk



Obrázek 15.7 Vytvoření uživatelského účtu — pravidla pro obsah WWW stránek

V sekci *Volby pro kontrolu obsahu WWW* je možné provést specifické nastavení filtrování obsahu WWW stránek pro konkrétního uživatele. Ve výchozím nastavení jsou všechny prvky povoleny. *WinRoute* umožňuje filtrování těchto prvků WWW stránek:

Objekty ActiveX
: Aktivní objekty na WWW stránkách. Tato volba povoluje / blokuje HTML tagy `<embed>` a `<object>`.

HTML tagy <script>
: Výkonný kód v jazycích *JavaScript*, *VBScript* atd.

Otevírání nových oken (pop-up windows)
: Automatické otevírání nových oken prohlížeče — typicky reklamy.
Tato volba povoluje / blokuje ve skriptech v jazyce *JavaScript* metodu *window.open()*.

HTML tagy <applet>
: Programy (tzv. applety) v jazyce *Java*.

Mezidoménové odkazy referer
: Povolení / blokování položky `Referer` v *HTTP* hlavičce.
Položka `Referer` obsahuje URL stránky, z níž klient na danou stránku přešel. Tato volba umožňuje blokovat položku `Referer` 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).

V sekci *Jazykové volby* lze nastavit preferovaný jazyk WWW rozhraní *WinRoute* (včetně rozhraní *Kerio StaR*). Volba *podle prohlížeče* znamená, že *WinRoute* detekuje nastavení preferovaných jazyků ve WWW prohlížeči uživatele a použije jazyk s nejvyšší preferencí, který má k dispozici. Není-li k dispozici žádný z preferovaných jazyků, bude použita angličtina.

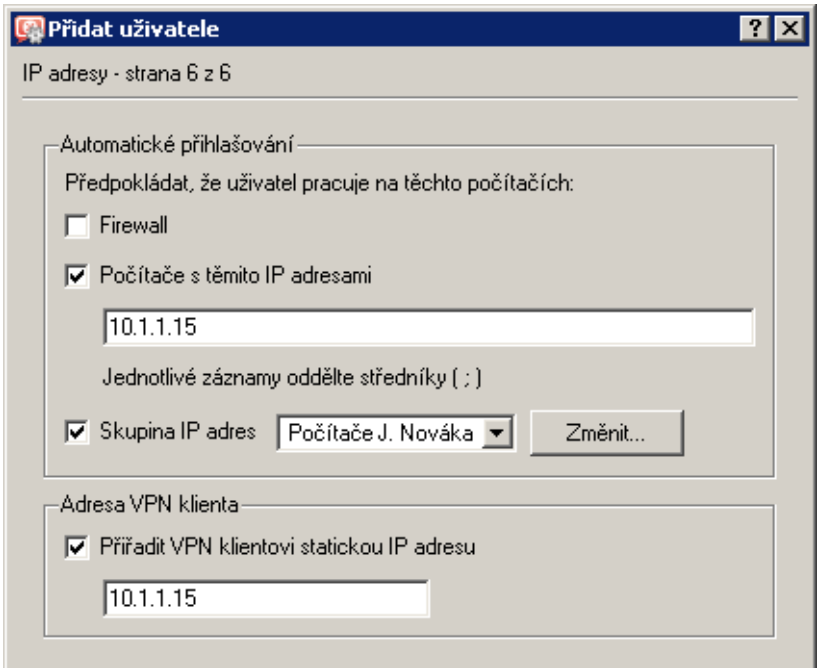
V preferovaném jazyce rovněž firewall zasílá uživateli e-mailové výstrahy (upozornění na překročení kvóty objemu přenesených dat, nalezený virus a detekci P2P sítě). Je-li jazyk nastavován podle preferencí ve WWW prohlížeči, pak bude použit preferovaný jazyk uživatele při posledním přihlášení do WWW rozhraní. Pokud uživatel dosud s WWW rozhraním nepracoval, budou výstrahy zasílány v angličtině.

Poznámka: Tato nastavení si uživatel může sám měnit na příslušné stránce WWW rozhraní *WinRoute* (viz manuál *Kerio WinRoute Firewall — Příručka uživatele*). Má-li uživatel právo „přejít pravidla pro obsah WWW stránek“, může nastavení měnit libovolně. V opačném případě může povolovat nebo zakazovat pouze ty prvky, které má v nastavení uživatelského účtu povoleny. Nastavení jazyka může měnit vždy.

Tip

Pravidla pro obsah WWW stránek mohou být nastavena šablonou uživatelského účtu.

Krok 6 — IP adresy uživatele



Obrázek 15.8 Vytvoření uživatelského účtu — IP adresy pro automatické přihlašování a VPN klienta

Pokud uživatel pracuje na vyhrazeném počítači (tj. nesdílí počítač s jinými uživateli) a tento počítač má pevnou IP adresou (statickou nebo rezervovanou na DHCP serveru), pak může být daný uživatel z této IP adresy automaticky ověřován. V praxi to znamená, že při zachycení komunikaci z této IP adresy *WinRoute* předpokládá, že se jedná o aktivitu majitele příslušného počítače, a nevyžaduje ověření uživatele. Vše (tj. pravidla pro přístup, sledování statistik atd.) pak funguje stejně, jako kdyby se uživatel přihlásil k firewallu svým uživatelským jménem a heslem.

Z výše uvedeného popisu logicky vyplývá, že z konkrétní IP adresy může být automaticky ověřován nejvýše jeden uživatel. *WinRoute* při definici uživatelského účtu kontroluje, zda není zadaná IP adresa již použita pro automatické ověřování jiného uživatele.

Automatické ověřování uživatele lze nastavit buď z firewallu (tj. počítače, na kterém je *WinRoute* nainstalován) nebo z libovolného jiného počítače, případně více počítačů (např. pokud má uživatel kromě své pracovní stanice také notebook). Pro specifikaci více počítačů lze využít skupinu IP adres (viz kapitola 14.1).

Upozornění

Automatické přihlašování uživatelů představuje určité bezpečnostní riziko. Pokud k počítači, ze kterého je uživatel automaticky ověřován, získá přístup neoprávněná osoba, pak může na tomto počítači pracovat pod identitou automaticky ověřeného uživatele. Automatické ověřování by mělo být doplněno ochranou — typicky ověřováním uživatele při přístupu do systému.

Sekce *Adresa VPN klienta* umožňuje nastavit IP adresu, která bude vždy přidělována VPN klientovi tohoto uživatele. Tímto způsobem lze zajistit, že i při přístupu do lokální sítě prostřednictvím aplikace *Kerio VPN Client* bude mít uživatel pevnou IP adresu. Tuto adresu pak můžeme přidat do seznamu IP adres, ze kterých bude uživatel automaticky přihlašován.

Podrobné informace o proprietárním VPN řešení firmy *Kerio Technologies* naleznete v kapitole 23.

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.

15.3 Lokální databáze uživatelů: externí ověřování a import účtů

Uživatelé v lokální databázi mohou být ověřováni v *Active Directory* doméně nebo v doméně *Windows NT* (viz kapitola 15.2, první krok průvodce). Pro použití těchto způsobů ověřování musí být počítač s *WinRoute* členem příslušné domény.

Je-li *WinRoute* nainstalován na systému *Windows*, musí lze počítač přidat do domény nebo změnit členství v doméně pouze v operačním systému (ve vlastnostech počítače).

V edici *Software Appliance / VMware* appliance je možné nastavit členství v doméně přímo ve správě firewallu:

- V rozhraní *Web Administration* v sekci *Domény a ověřování*, záložka *Active Directory*,
- V programu *Administration Console* v sekci *Uživatelé*, záložka *Active Directory*.

WinRoute v edici *Software Appliance / VMware Virtual Appliance* lze připojit pouze do domény *Active Directory*, nikoliv do domény *Windows NT*.

Import uživatelských účtů

Do lokální databáze uživatelů lze importovat vybrané účty z domény *Active Directory* nebo *Windows NT* (import z domény *Windows NT* je možný pouze ve *WinRoute* na systému *Windows*).

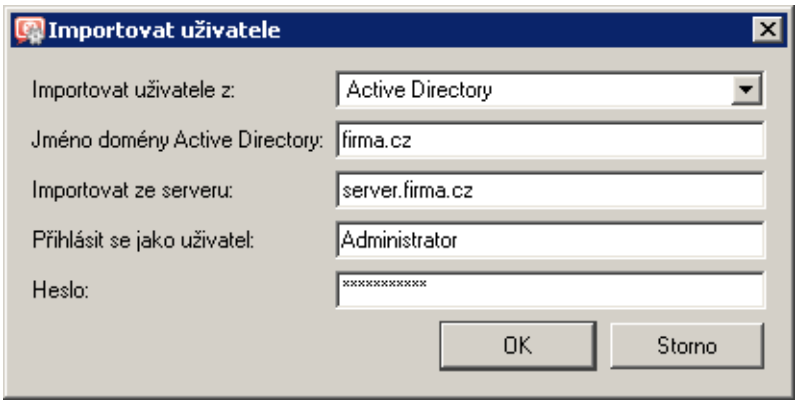
Import uživatelského účtu znamená vytvoření lokálního účtu se stejným uživatelským jménem a ověřováním v příslušné doméně. Specifické parametry pro *WinRoute* (např. přístupová práva, pravidla pro obsah WWW stránek, kvóty objemu přenesených dat apod.) budou nastaveny podle šablony pro lokální databázi uživatelů (viz kapitola 15.1), případně je lze u vybraných účtů nastavit individuálně. U všech importovaných účtů bude nastaven typ ověřování *Active Directory / Windows NT*.

Poznámka: Tento způsob importu uživatelských účtů je vhodný zejména při použití *Windows NT* domény (doménový server s operačním systémem *Windows NT Server*). V případě *Active Directory* domény je výhodnější a jednodušší je použít transparentní podporu *Active Directory* (mapování domény — viz kapitola 15.4).

Import uživatelských účtů se provede stisknutím tlačítka *Importovat* pod seznamem uživatelských účtů (v položce *Doména* musí být zvolena *Lokální databáze uživatelů*, jinak je toto tlačítko neaktivní).

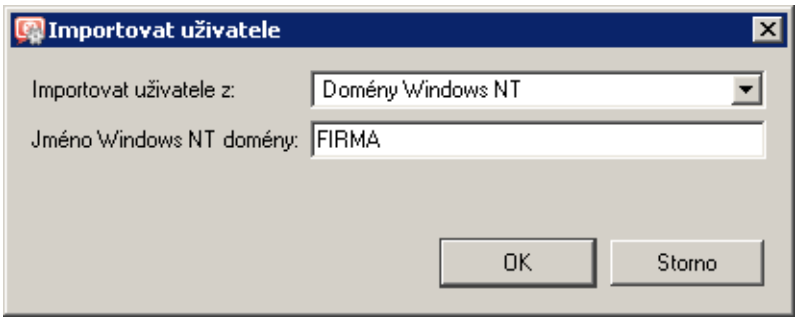
V dialogu pro import účtů je nejprve třeba zvolit typ domény, z níž mají být účty importovány, a podle typu domény pak zadat příslušné parametry:

- *Active Directory* — pro import účtů musí být zadáno jméno *Active Directory* domény, DNS jméno nebo IP adresa doménového serveru a přihlašovací údaje pro čtení databáze uživatelů (libovolný uživatelský účet z příslušné domény).



Obrázek 15.9 Import účtů z Active Directory

- *NT doména* — pro import účtů musí být zadáno jméno domény. Počítač s *WinRoute* musí být členem této domény.



Obrázek 15.10 Import účtů z domény Windows NT

Poznámka: Import uživatelských účtů z domény *Windows NT* lze provést pouze ve *WinRoute* na operačním systému *Windows*.

Po úspěšném spojení s příslušným doménovým serverem se zobrazí seznam všech účtů v zadané doméně. Po výběru požadovaných účtů a potvrzení dialogu budou účty importovány do lokální databáze uživatelů.

15.4 Uživatelské účty v Active Directory — mapování domén

Ve *WinRoute* lze přímo používat uživatelské účty z jedné nebo více *Active Directory* domén. Tato funkce se nazývá transparentní podpora *Active Directory* nebo též mapování *Active Directory* domén. Hlavní výhodou je, že veškerá správa uživatelských účtů a skupin probíhá pouze v databázi *Active Directory* (s použitím standardních systémových nástrojů). Ve *WinRoute* lze pro každou doménu definovat šablonu, podle které budou nastaveny specifické parametry účtů pro *WinRoute* (přístupová práva, kvóty objemu dat a pravidla pro obsah WWW stránek — viz kapitola 15.1). V případě potřeby lze u konkrétních účtů tyto parametry nastavit individuálně.

Poznámka: Doménu *Windows NT* nelze popsaným způsobem mapovat. V případě *Windows NT* domény doporučujeme importovat uživatelské účty do lokální databáze uživatelů (viz kapitola 15.3)

Podmínky použití mapovaných domén

Pro správnou funkci ověřování uživatelů v mapovaných *Active Directory* doménách musí být splněny tyto podmínky:

- V případě jedné mapované domény:
  1. Počítač s *WinRoute* musí být členem příslušné *Active Directory* domény.
  2. Počítače v lokální síti (pracovní stanice uživatelů) by měly jako primární DNS server používat *DNS forwarder* ve *WinRoute*, který dokáže zpracovat dotazy do *Active Directory* a předat je příslušnému doménovému serveru. Při použití jiného DNS serveru nelze zaručit správnou funkčnost ověřování uživatelů v *Active Directory*.
- V případě mapování více domén:

1. Počítač s *WinRoute* musí být členem jedné z mapovaných domén. Tato doména bude označována jako primární.
2. Primární doména musí důvěřovat všem ostatním doménám, které jsou ve *WinRoute* mapovány (podrobnosti viz dokumentace k operačnímu systému na příslušném doménovém serveru).
3. Pro nastavení DNS platí stejná pravidla jako v případě mapování jedné domény (nejvhodnější je použít *DNS forwarder* ve *WinRoute*).

Nastavení mapování domén

Mapování *Active Directory* domén lze nastavit:

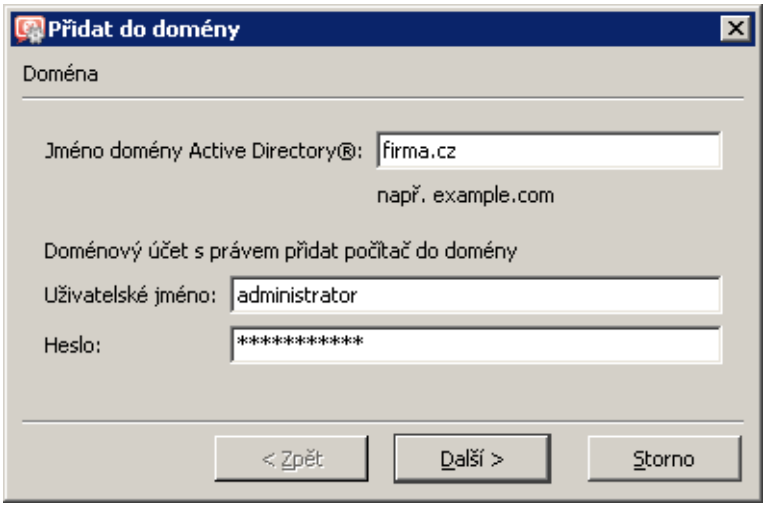
- v programu *Administration Console* v sekci *Uživatelé a skupiny* → *Uživatelé*, záložka *Active Directory*,
- v rozhraní *Web Administration* v sekci *Uživatelé a skupiny* → *Domény a ověřování*, záložka *Active Directory*.

Připojení firewallu do domény (Software Appliance / VMware Virtual Appliance)

Horní část záložky *Active Directory* zobrazuje informaci o členství počítače s firewallem v doméně.

V edici *Software Appliance / VMware Virtual Appliance* je možné firewall přidat do domény, změnit členství v doméně nebo odpojit od domény.

Přidat firewall do domény nebo změnit jeho členství v doméně lze pomocí jednoduchého průvodce.



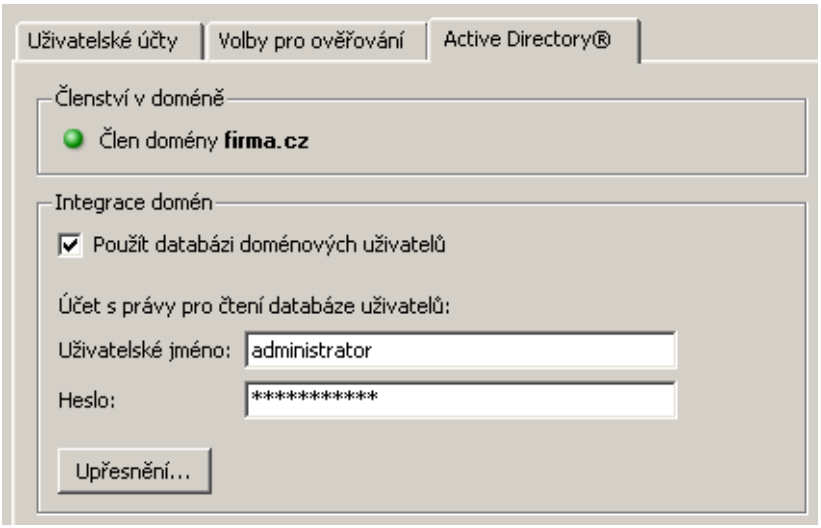
Obrázek 15.11 Přidání firewallu do domény

V prvním kroku průvodce je potřeba zadat celé jméno domény *Active Directory* (např. `firma.cz`) a jméno a heslo uživatele s právem přidávat počítače do domény.

Pokud se *WinRoute* nepodaří automaticky nalézt doménový server zadané domény, dotáže se v dalším kroku na jeho IP adresu. Poté bude uživatel informován o výsledku přidání firewallu do domény.

Mapování primární domény

Mapování primární domény (tedy domény, které je počítač s firewallem členem), nastavíme volbou *Použít databázi doménových uživatelů*. Pro připojení k doménovému serveru je potřeba zadat uživatelské jméno a heslo s právy pro čtení databáze uživatelů (lze použít libovolný uživatelský účet z příslušné domény, není-li zablokován).



Obrázek 15.12 Mapování primární domény

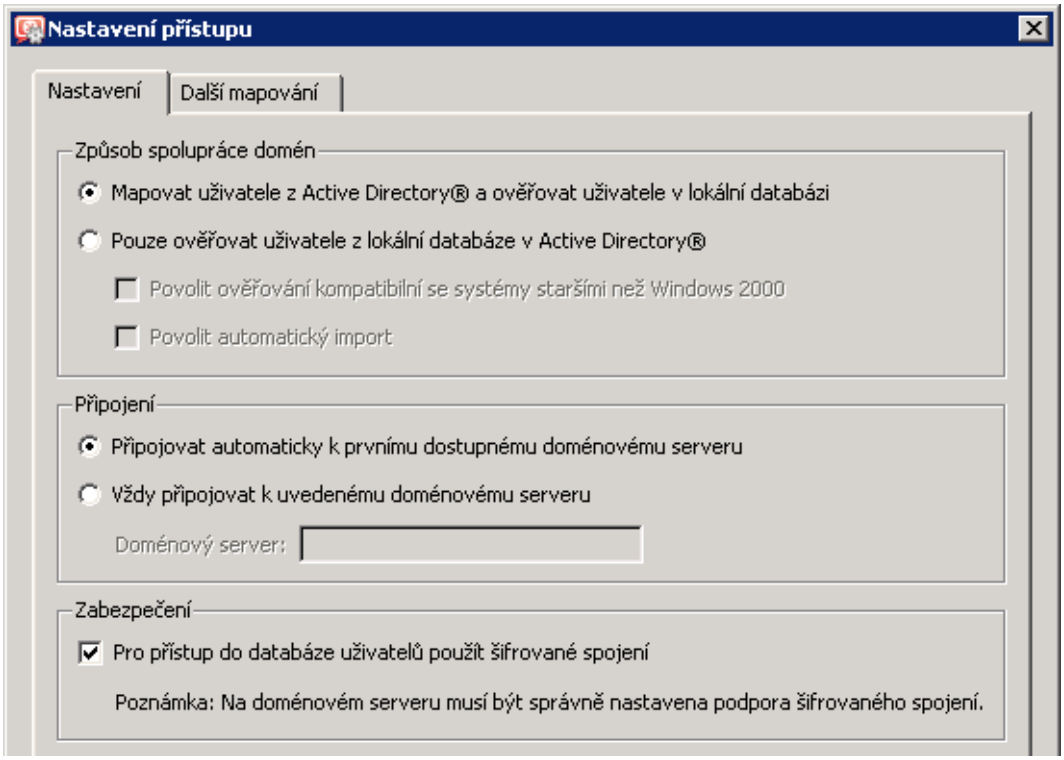
Upřesňující nastavení

Způsob spolupráce *WinRoute* s *Active Directory* lze ovlivnit několika upřesňujícími parametry.

Mapování domény versus ověřování uživatelů v doméně

Doporučený způsob spolupráce s *Active Directory* je mapování domény (uživatelské účty jsou uloženy a spravovány pouze v *Active Directory*). Toto však v určitých situacích nemusí být žádoucí. Např. při nasazení *Active Directory* do sítě, kde byla dříve používána doména *Windows NT* nebo kde nebyla použita žádná doména, jsou již účty uživatelů vytvořeny v lokální databázi *WinRoute*. V takovém případě je nejjednodušším řešením zachovat lokální účty a pouze nastavit ověřování v *Active Directory* (aby uživatelé měli shodné heslo do domény i na firewall).

Je-li *WinRoute* nainstalován na systému *Windows*, pak je možné povolit ověřování kompatibilní se staršími systémy (tzn. ověřování v doméně *Windows NT*). Tuto volbu je nutné zapnout v případě, že doménový server používá operační systém *Windows NT* nebo některý z klientů v lokální síti používá operační systém *Windows* starší než *Windows 2000*.



Obrázek 15.13 Upřesňující nastavení spolupráce s Active Directory

V *Software Appliance / VMware Virtual Appliance* tato volba není k dispozici (ověřování v doméně *Windows NT* není podporováno).

Dále je k dispozici volba pro automatický import uživatelských účtů z *Active Directory* do lokální databáze (po prvním přihlášení uživatele k firewallu doménovým jménem a heslem bude automaticky vytvořen účet stejného jména v lokální databázi). Tato volba slouží výhradně pro zachování kompatibility se staršími verzemi *WinRoute*. V nových instalacích je jednoznačně doporučeno použít mapování domén — správa uživatelů je pak výrazně jednodušší a méně časově náročná. Bližší informace naleznete v *Příručce Administrátora* ke starším verzím *WinRoute* (verze *6.7.0* nebo nižší).

Výběr doménového serveru

Ve výchozím nastavení *WinRoute* detekuje automaticky doménové servery pro zadanou doménu a pro komunikaci s databází *Active Directory* použije první nalezený server. Automatická detekce výrazně zjednodušuje konfiguraci (není nutné zadávat IP adresy jednotlivých doménových serverů).

V případě potřeby můžeme zadat jméno nebo IP adresu konkrétního doménového serveru. *WinRoute* pak nebude provádět automatickou detekci a bude se vždy připojovat pouze k zadanému serveru.

Zabezpečené připojení k doménovému serveru

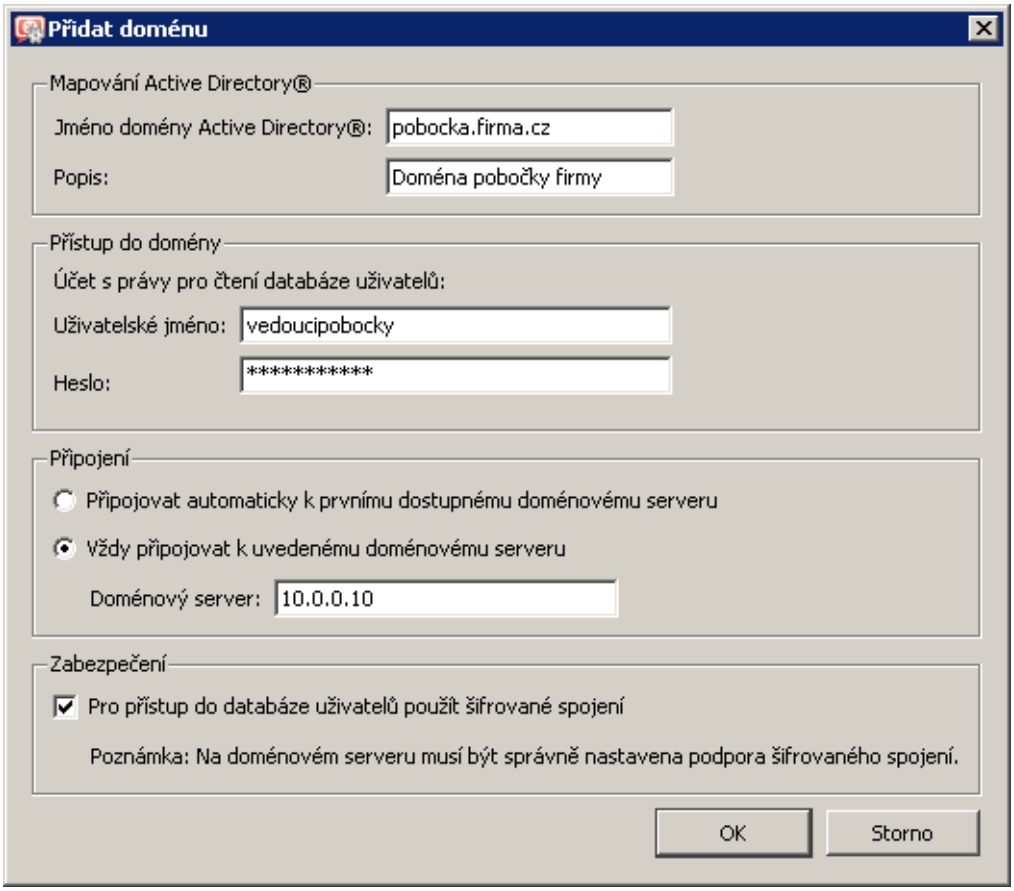
Pro zvýšení bezpečnosti (znemožnění odposlechu komunikace a získání hesel uživatelů) může být komunikace se serverem *Active Directory* šifrována. Povolení šifrovaného spojení vyžaduje odpovídající nastavení na příslušném doménovém serveru (resp. na všech

serverech dané domény, pokud je použita automatická detekce).

Mapování dalších domén

Chceme-li mapovat uživatelské účty z několika různých *Active Directory* domén, přidáme další domény v upřesňujících nastaveních na záložce *Další mapování*.

Uživatelé z ostatních domén musí při přihlašování zadávat své uživatelské jméno včetně domény (např. `pmaly@pobocka.firma.cz`). Uživatelské účty, u nichž není specifikována doména (např. `jnovak`), budou hledány v primární doméně nebo v lokální databázi.



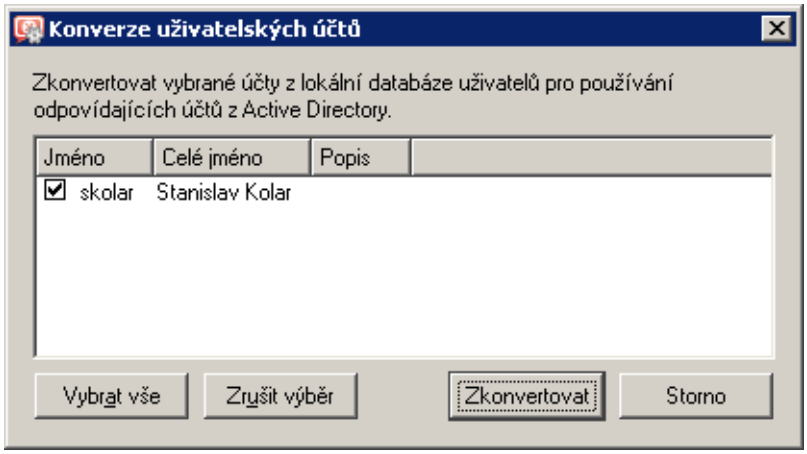
Obrázek 15.14 Přidání další domény Active Directory

Tlačítko *Přidat* nebo *Změnit* otevírá dialog pro definici domény, ve kterém lze zadat parametry mapované domény. Podrobnosti viz výše (mapování primární domény a upřesňující nastavení).

Konflikt Active Directory s lokální databází a konverze účtů

Při mapování *Active Directory* domény může dojít ke konfliktu s lokální databází uživatelů, pokud v doméně i v lokální databázi existuje uživatelský účet stejného jména. Je-li mapováno více domén, může konflikt nastat pouze mezi lokální databází a primární doménou (účty z ostatních domén musí být vždy uváděny včetně domény, čímž je konflikt vyloučen).

V případě konfliktu se v dolní části záložky *Uživatelské účty* zobrazí příslušné varování. Kliknutím na odkaz ve varovné zprávě lze provést tzv. konverzi vybraných uživatelských účtů (nahrazení lokálních účtů odpovídajícími účty z *Active Directory*).



Obrázek 15.15 Konverze uživatelských účtů

Při konverzi účtu budou automaticky provedeny tyto operace:

- nahrazení všech výskytů lokálního účtu v konfiguraci *WinRoute* (v komunikačních pravidlech, pravidlech pro URL, pravidlech pro FTP atd.) odpovídajícím účtem z *Active Directory* domény,
- odstranění účtu z lokální databáze uživatelů.

Účty, které nebudou vybrány pro konverzi, zůstanou v lokální databázi uživatelů zachovány (a nadále bude hlášen konflikt). Konfliktní účty lze používat — jedná se o dva nezávislé účty. Účet z *Active Directory* však musí být vždy zadáván včetně domény (přestože se jedná o primární doménu); uživatelské jméno bez domény představuje účet z lokální databáze. Je-li to však možné, doporučujeme všechny konflikty odstraňovat konverzí příslušných účtů.

Poznámka: V případě skupin uživatelů ke konfliktům nedochází — lokální skupiny jsou vždy nezávislé na *Active Directory* (i v případě, že je jméno lokální skupiny shodné se jménem skupiny v příslušné doméně).

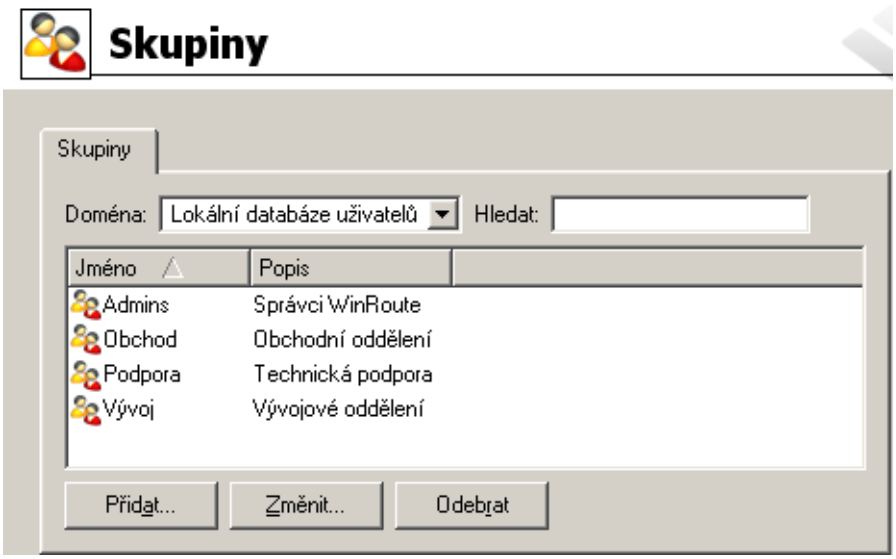
15.5 Skupiny uživatelů

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).

Definice skupin uživatelů

Skupiny uživatelů se definují v sekci *Uživatelé a skupiny* → *Skupiny*.



Obrázek 15.16 Skupiny uživatelů ve WinRoute

Doména

Volba *Doména* umožňuje vybrat doménu, pro kterou budeme definovat skupiny uživatelů nebo nastavovat jejich parametry. V této položce lze zvolit některou z mapovaných *Active Directory* domén (viz kapitola 15.4) nebo lokální databázi uživatelů.

Ve *WinRoute* lze vytvářet skupiny pouze v lokální databázi uživatelů. Nelze je vytvářet v mapovaných *Active Directory* doménách. Rovněž není možné importovat skupiny z domény *Windows NT* nebo *Active Directory* do lokální databáze.

V případě skupin v mapovaných *Active Directory* doménách lze pouze nastavit přístupová práva (viz dále — 3. krok průvodce vytvořením skupiny uživatelů).

Vyhledávání

Funkce *Hledat* umožňuje zadat filtr pro zobrazení skupin uživatelů.

Vyhledávání je interaktivní — s každým zadaným (resp. smazaným) znakem se zobrazí všechny skupiny obsahující zadaný řetězec znaků v položce *Jméno* nebo *Popis*. Kliknutím na ikonu vedle pole pro zadání hledaného řetězce se filtr zruší a zobrazí se všechny skupiny ve vybrané doméně (pokud je pole *Hledat* prázdné, ikona pro zrušení filtru je skryta).

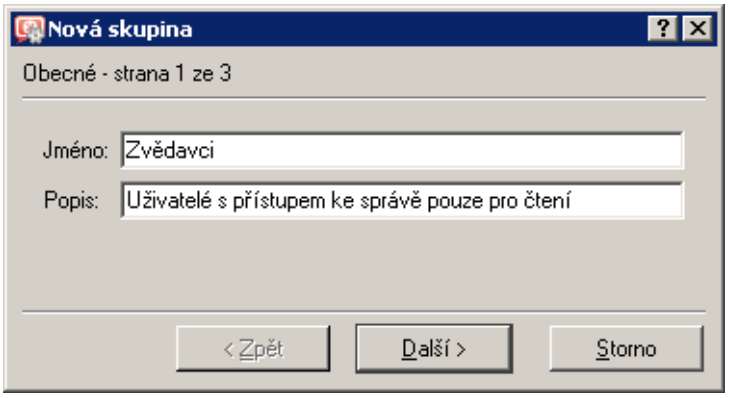
Vyhledávání je užitečné zejména při velkém počtu skupin, kdy by nalezení požadované skupiny klasickou cestou bylo značně zdlouhavé.

Vytvoření lokální skupiny uživatelů

V položce *Doména* v sekci *Skupiny* zvolíme lokální databázi uživatelů.

Novou skupinu uživatelů vytvoříme pomocí původce, který se zobrazí po stisknutí tlačítka *Přidat*.

Krok 1 — název a popis skupiny

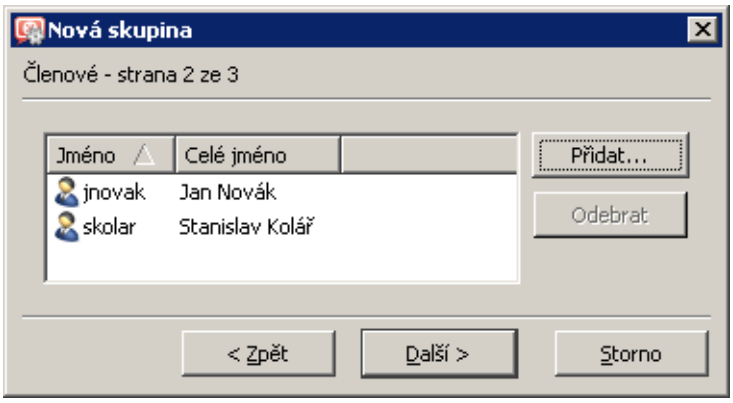


Obrázek 15.17 Vytvoření skupiny uživatelů — základní parametry

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



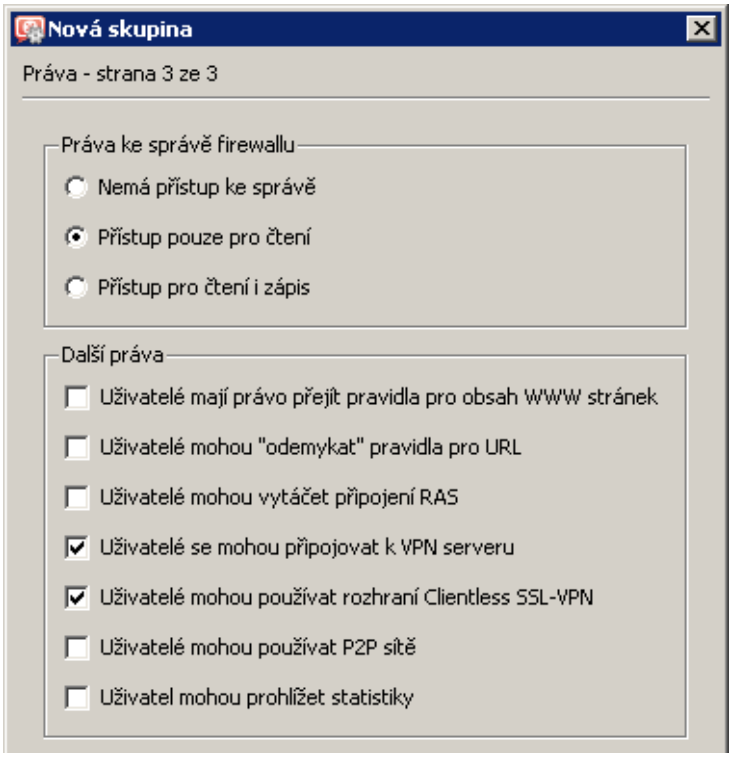
Obrázek 15.18 Vytvoření skupiny uživatelů — zařazení uživatelských účtů do skupiny

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 15.1).

Tip

Při přidávání uživatelů lze označit více uživatelských účtů najednou přidržením klávesy *Ctrl* nebo *Shift*.

Krok 3 — uživatelská práva členů skupiny



Obrázek 15.19 Vytvoření skupiny uživatelů — uživatelská práva členů 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.

Doplňková práva:

Uživatelé mají právo přejít pravidla...
: Tato volba umožňuje členům skupiny měnit osobní nastavení filtrování obsahu WWW stránek (viz kapitola 15.2).

Uživatelé mohou „odemykat“ pravidla pro URL
: Tato volba povoluje členům skupiny jednorázově obejít zákaz přístupu na blokované WWW stránky (pokud to povoluje příslušné pravidlo pro URL — viz kapitola 12.2). Všechna „odemknutí“ budou zaznamenána do záznamu *Security*.

Uživatelé mohou vytáčet připojení RAS
: Pokud je připojení k Internetu realizováno vytáčenými linkami, uživatelé z této skupiny budou moci tyto linky vytáčet a zavěšovat prostřednictvím WWW rozhraní firewallu (viz kapitola 11).

Uživatelé se mohou připojovat k VPN serveru
: Členové skupiny se mohou připojovat přes Internet do lokální sítě prostřednictvím aplikace *Kerio VPN Client* (podrobnosti viz kapitola 23).

Uživatelé mohou používat rozhraní Clientless SSL-VPN
: Členové této skupiny budou moci přistupovat ke sdíleným souborů a složkám v lokální síti prostřednictvím webového rozhraní *Clientless SSL-VPN*.
Rozhraní *Clientless SSL-VPN* a příslušné uživatelské právo je k dispozici pouze ve *WinRoute* pro systém *Windows*. Podrobnosti viz kapitola 24.

Uživatelé mohou používat P2P sítě
: Na členy této skupiny nebude aplikován modul *P2P Eliminator* (detekce a blokování *Peer-to-Peer* sítí — viz kapitola 17.1).

Uživatelé mohou prohlížet statistiky
: Členové této skupiny budou mít přístup ke statistikám firewallu zobrazovaným ve WWW rozhraní (viz kapitola 11).

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 16

Administrativní nastavení

16.1 Systémová konfigurace (Software Appliance / VMware Virtual Appliance)

V edici *Software Appliance / VMware Virtual Appliance* umožňuje konzole pro správu *WinRoute* také nastavení některých základních parametrů operačního systému firewallu. Tato nastavení jsou nutná pro správnou činnost firewallu a jsou umístěna v sekci *Konfigurace / Další volby*, záložka *Systémová konfigurace*.

Obrázek 16.1 Systémová konfigurace — jméno počítače, datum, čas a časová zóna

Jméno serveru

Nastavení jména serveru je důležité pro některé služby *WinRoute* (např. zabezpečené WWW rozhraní), ale i pro služby operačního systému firewallu.

Modul *DNS forwarder* ve *WinRoute* zadanému jménu automaticky přiřadí IP adresy všech rozhraní firewallu. Pokud je v lokální síti použit jiný DNS server, pak je potřeba na něm nastavit odpovídající DNS záznamy.

Datum, čas a časová zóna

Pro celou řadu funkcí *WinRoute* (ověřování uživatelů, statistiky, záznamy atd.) je nutné správné nastavení data, času a časové zóny.

Datum a čas lze nastavit ručně, vhodnější je však využít NTP server, který poskytuje informaci o přesném čase a umožňuje automaticky korigovat systémový čas firewallu. Nastavená časová zóna rovněž poskytuje informaci o letním a zimním čase.

Společnost *Kerio Technologies* pro tento účel nabízí několik volně přístupných NTP serverů: `0.kerio.pool.ntp.org`, `1.kerio.pool.ntp.org`, `2.kerio.pool.ntp.org` a `3.kerio.pool.ntp.org`.

16.2 Nastavení vzdálené správy

Vzdálená správa znamená připojení k firewallu, sledování jeho stavu a provádění konfiguračních změn pomocí programu *Administration Console* nebo rozhraní *Web Administration* z jiného počítače, než na kterém je *WinRoute* nainstalován.

Obsahuje-li *WinRoute* pouze komunikační pravidla vytvořená automaticky pomocí průvodce (viz kapitola 7.1), pak je přístup ke vzdálené správě povolen přes všechna důvěryhodná síťová rozhraní (viz kapitola 5). Prakticky to znamená, že vzdálená správa je povolena ze všech počítačů v lokální síti.

Povolení či zákaz vzdálené správy z Internetu (resp. z nedůvěryhodných sítí) se provádí definicí odpovídajícího komunikačního pravidla. Komunikace mezi *WinRoute* a programem *Administration Console* probíhá protokoly TCP a UDP na portu `44333`. Pro tento účel je ve *WinRoute* předdefinována služba *KWF Admin*. Zabezpečená verze rozhraní *Web Administration* používá protokol TCP, ve výchozím nastavení na portu `4081` — předdefinovaná služba *KWF WebAdmin-SSL*.

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 (viz kapitola 14.1).
  Z bezpečnostních důvodů nedoporučujeme povolovat vzdálenou správu z libovolného počítače v Internetu (tj. nastavovat *Zdroj* = *Libovolný* nebo *Zdroj* = *Internet*)!
- *Cíl* — *Firewall* (tj. počítač, na němž je *WinRoute* nainstalován).
- *Služba* — *KWF Admin* (připojení programem *Administration Console*) a *KWF WebAdmin-SSL* (zabezpečená verze rozhraní *Web Administration*).
  Nedoporučujeme povolovat přístup k nezabezpečené verzi rozhraní *Web Administration* (služba *KWF WebAdmin*)! Nezabezpečená komunikace může být odposlouchávána a zneužita k napadení firewallu a počítačů v lokální síti.
- *Akce* — *Povolit* (jinak by vzdálená správa byla i nadále blokována).
- *Překlad* — nepřekládat zdrojovou ani cílovou adresu (tzn. nenastavovat žádný překlad adres).

Jméno	Zdroj	Cíl	Služba	Akce	Překlad
☑ Vzdálená správa WinRoute	Vzdálená správa	Firewall	KWF Admin KWF WebAdmin-SSL	✓	

Obrázek 16.2 Komunikační pravidlo pro povolení vzdálené správy

Tip

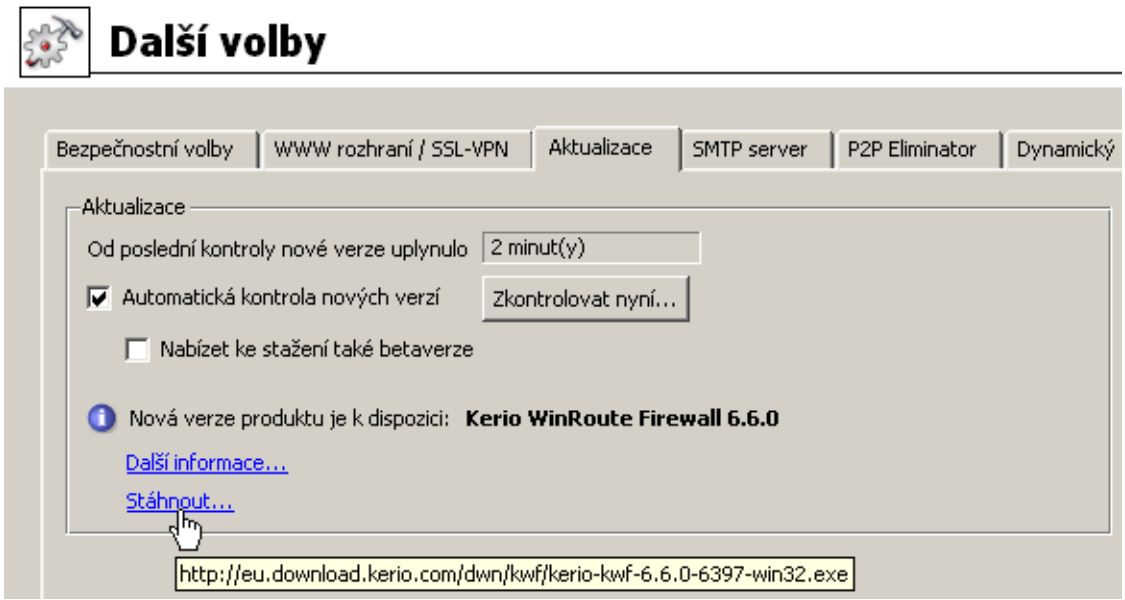
Obdobným způsobem lze ve *WinRoute* povolit či zakázat vzdálenou správu produktu *Kerio MailServer* — pro připojení programem *Administration Console* využijeme předdefinovanou službu *KMS Admin*, pro rozhraní *Web Administration* službu *HTTPS*.

Poznámka: Nesprávnou definicí komunikačního pravidla je možné zablokovat vzdálenou správu z počítače, z něhož ji právě provádíte. *WinRoute* však ve většině případů tuto situaci detekuje a zobrazí varování. Lokální připojení (tj. přímo z počítače, na němž běží *WinRoute Firewall Engine*) ale funguje vždy. Tuto komunikaci nelze zablokovat žádným pravidlem.

16.3 Automatická aktualizace produktu

WinRoute může v pravidelných intervalech kontrolovat, zda se na serveru firmy Kerio Technologies nachází novější verze produktu, než je aktuálně nainstalována. Pokud ano, nabídne její stažení a instalaci.

V sekci *Konfigurace* → *Další volby*, záložka *Aktualizace* lze zjistit informace o nové verzi a nastavit parametry automatické kontroly nových verzí.



Obrázek 16.3 Kontrola nových verzí WinRoute

Od poslední kontroly nové verze uplynulo

V tomto poli se zobrazuje doba, která uplynula od posledního pokusu o aktualizaci *WinRoute*.

Příliš dlouhá doba (několik dní) může indikovat, že automatická kontrola nové verze z nějakého důvodu selhává (typickým příkladem je blokování přístupu na aktualizační server komunikačními pravidly). V takovém případě doporučujeme zkusit provést aktualizaci ručně (stisknutím tlačítka *Zkontrolovat nyní*), prohlédnout si zprávu o výsledku v záznamu *Debug* (viz kapitola 22.6) a provést příslušná opatření.

Provádět kontrolu nových verzí

Tato funkce zapíná/vypíná automatickou kontrolu nových verzí. Kontrola se provádí:

- 2 minuty po každém startu *WinRoute Firewall Engine*,
- dále každých 24 hodin.

Výsledek každého pokusu o aktualizaci *WinRoute* (úspěšného i neúspěšného) je zapsán do záznamu *Debug* (viz kapitola 22.6).

Nabízet ke stažení také betaverze

Po zapnutí této volby budou při kontrole nových verzí nabízeny ke stažení a instalaci také betaverze *WinRoute*.

Pokud se chcete podílet na testování betaverzí, zaškrtněte tuto volbu. V případě, že je *WinRoute* nasazen v ostrém provozu (např. na internetové bráně vaší firmy), nedoporučujeme betaverze instalovat — nezapínejte volbu *Nabízet ke stažení betaverze*.

Zkontrolovat nyní

Toto tlačítko spustí okamžitou kontrolu nové verze.

V případě nalezení nové verze jsou nabídnuty odkazy pro podrobné informace a stažení instalačního souboru:

- *Další informace* — tento odkaz otevře ve výchozím WWW prohlížeči stránku s historií verzí (changelogem) *WinRoute*.
- *Stáhnout* — přímý odkaz na instalační soubor příslušné verze. Kliknutím bude zahájeno stahování instalačního souboru ve výchozím prohlížeči.

Podrobnosti o instalaci *WinRoute* naleznete v kapitole 2.4.

Poznámka: Je-li zjištěna nová verze, pak se tato informace zobrazuje také jako odkaz na úvodní stránce administračního okna (obrázek s informacemi o aplikaci a licenci). Kliknutím na odkaz se *Administration Console* přepne do sekce *Konfigurace* → *Další volby*, záložka *Aktualizace*.

Kapitola 17

Doplňkové bezpečnostní funkce

17.1 Detekce a blokování P2P sítí

Peer-to-Peer sítě (zkr. *P2P* sítě) je označení pro celosvětové distribuované systémy, ve kterých může každý uzel sloužit zároveň jako klient i jako server. Tyto sítě slouží ke sdílení velkého objemu dat mezi uživateli (většinou soubory s nelegálním obsahem). Typickými představiteli těchto sítí jsou např. *DirectConnect* nebo *Kazaa*.

Používání *P2P* sítí jednak napomáhá šíření nelegálních souborů, ale zejména značně zatěžuje linku, kterou je uživatel připojen k Internetu. Pokud se takový uživatel nachází v lokální síti, která je připojena k Internetu jedinou linkou, pak jsou jeho aktivity na úkor ostatních uživatelů, případně i zvýšených nákladů na připojení (např. jedná-li se o linku s limitem přenesených dat).

WinRoute obsahuje modul *P2P Eliminator*, který umožňuje detekovat přístup do *P2P* sítí a provádět určitá opatření vůči příslušným uživatelům. Vzhledem k tomu, že *P2P* sítí existuje velké množství a uživatelé mohou na svých uzlech měnit řadu parametrů (např. porty pro server, počet spojení atd.), nelze jejich používání vždy s určitostí detekovat[6]. *P2P Eliminator* na základě určitých charakteristických znaků (známé porty, otevřená spojení atd.) vyhodnotí, že uživatel pravděpodobně používá jednu nebo více *P2P* sítí.

Na uživatele *P2P* sítí (tzn. na počítače, na nichž jsou klienti těchto sítí provozováni) je možné aplikovat tyto typy omezení:

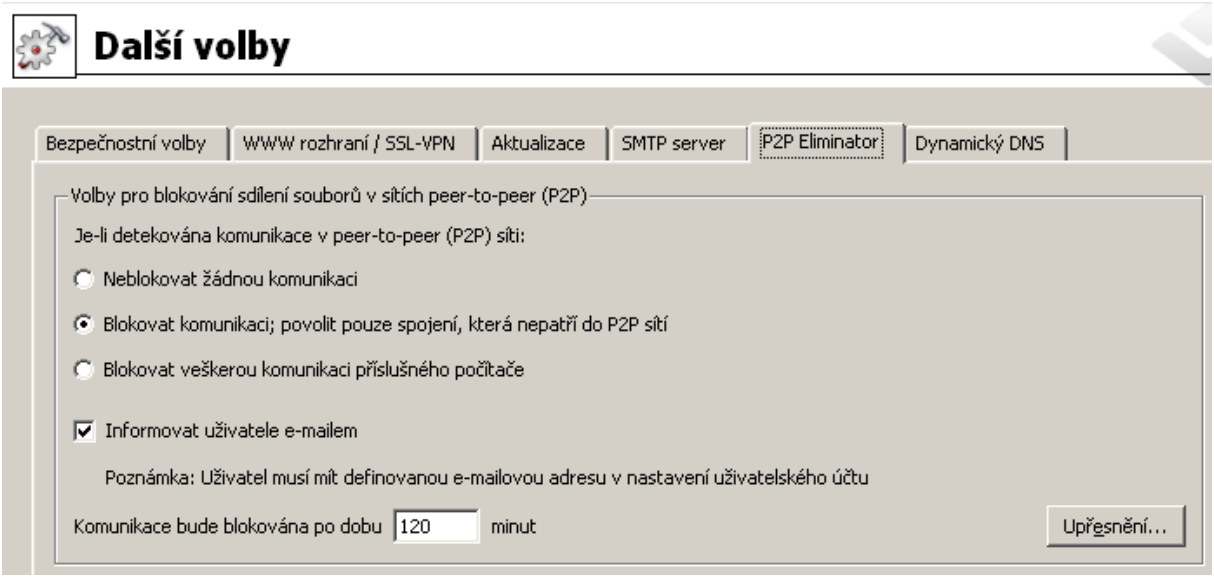
- *Blokování komunikace* — příslušnému počítači může být zcela zablokován přístup do Internetu nebo povolen přístup pouze k některým službám (např. WWW a e-mail),
- *Omezení šířky pásma* — klientům *P2P* sítí lze omezit rychlost přenosu dat tak, aby nedocházelo ke zbytečnému zatěžování internetové linky na úkor ostatních uživatelů a služeb.

Nastavení modulu P2P Eliminator

Detekce *P2P* sítí probíhá automaticky (modul *P2P Eliminator* je stále aktivní). Parametry modulu *P2P Eliminator* lze nastavit v sekci *Konfigurace* → *Další volby*, záložka *P2P Eliminator*.

Z výše uvedeného popisu vyplývá, že není technicky možné blokovat přístup do konkrétní *P2P* sítě. *P2P Eliminator* umožňuje kompletně zablokovat veškerou komunikaci (tj. přístup do Internetu z daného počítače), povolit pouze služby, které bezpečně nepatří do P2P sítí, nebo omezit šířku pásma (přenosovou rychlost), kterou mohou klienti *P2P* sítí využívat. Nastavené omezení bude vždy aplikováno na všechny klienty *P2P* sítí, které *P2P Eliminator* detekuje.

[6] Důkladné testy však prokázaly, že úspěšnost této detekce je velmi vysoká.

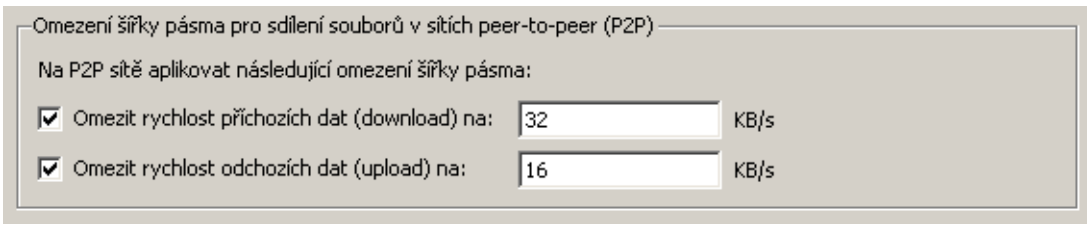


Obrázek 17.1 Nastavení detekce a blokování P2P sítí

Po zapnutí volby *Informovat uživatele e-mailem* bude uživateli přihlášenému z počítače, na kterém byl detekován klient *P2P* sítě, zaslán e-mail s varováním a informací o provedeném opatření (blokování veškeré komunikace / povolení pouze určitých služeb a doba trvání tohoto omezení). E-mail je samozřejmě zaslán pouze v případě, že je v příslušném uživatelském účtu uvedena platná e-mailová adresa (viz kapitola 15.1). Na nepřihlášené uživatele nemá tato volba žádný vliv.

Parametr *Komunikace bude blokována ...* určuje dobu, na po kterou bude příslušné omezení daného počítače platit. Modul *P2P Eliminator* po této době blokování zruší — není nutný zásah administrátora *WinRoute*. Doba blokování komunikace by měla být dostatečně dlouhá, aby si uživatel uvědomil následky své činnosti a nepokoušel se znovu připojovat k *P2P* sítím.

Není-li komunikace klientů *P2P* sítí blokována, pak je možné v dolní části záložky *P2P Eliminator* nastavit omezení šířky pásma pro *P2P* sítě. Internetové linky bývají zpravidla asymetrické (různá rychlost v příchozím a v odchozím směru), a proto se toto omezení nastavuje pro každý směr přenosu dat odděleně. Omezení šířky pásma má vliv pouze na komunikaci v rámci *P2P* sítí (detekovaných modulem *P2P Eliminator*), ostatní služby nejsou omezovány.



Obrázek 17.2 Omezení šířky pásma pro P2P sítě

Poznámka:

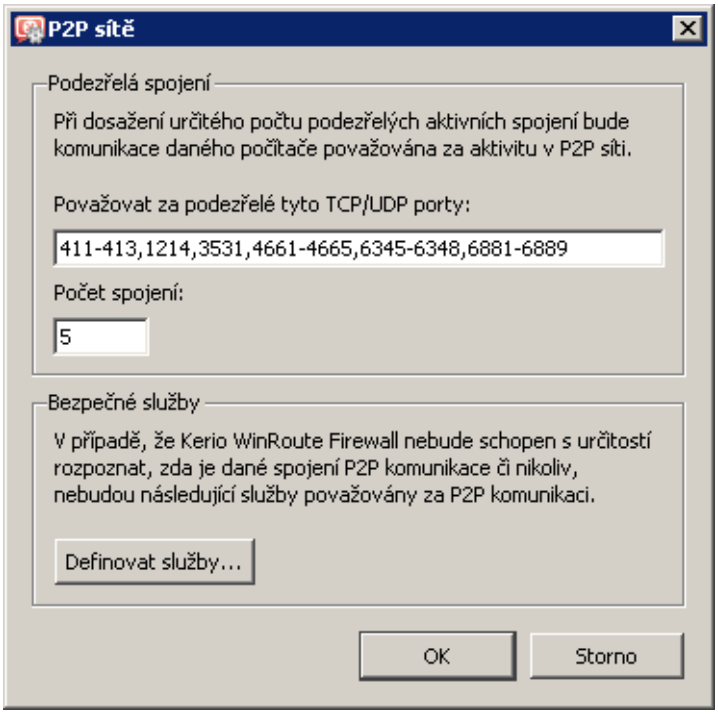
1. Je-li z určitého počítače k firewallu přihlášen uživatel, který má právo používat *P2P* sítě (viz kapitola 15.1), pak při detekci *P2P* sítě nejsou na tento počítač aplikována žádná omezení. Pro nepřihlášené uživatele platí vždy volby nastavené v záložce *P2P Eliminator*.

2. Informace o detekci *P2P* sítí a blokování komunikace se zobrazují v sekci *Stav* → *Počítače / uživatelé* (podrobnosti viz kapitola 19.1).

3. Chceme-li při detekci *P2P* zasílat e-mail jiné osobě (např. správci *WinRoute*), můžeme definovat příslušnou výstrahu v sekci *Konfigurace* → *Statistiky a záznamy*, záložka *Nastavení výstrah*. Podrobnosti viz kapitola 19.4.

Parametry pro detekci P2P sítí

Tlačítko *Upřesnění* otevírá dialog pro nastavení parametrů detekce *P2P* sítí.



Obrázek 17.3 Definice parametrů detekce P2P sítí

Porty P2P sítí

Seznam portů, o nichž je ověřeno, že jsou používány výhradně aplikacemi pro *P2P sítě*. Jedná se zpravidla o porty pro řídicí spojení — porty (resp. rozsah portů) pro sdílení souborů si většinou může každý uživatel nastavit téměř libovolně.

Do seznamu portů lze zadávat čísla portů nebo rozsahy portů. Jednotlivé hodnoty se oddělují čárkami, pro zápis rozsahu se používá pomlčka.

Počet podezřelých spojení

Pro *P2P* sítě je typický velký počet navázaných spojení z klientského počítače (zpravidla jedno spojení pro každý soubor). Parametr *Počet spojení* určuje minimální počet síťových spojení klienta, při kterém bude jeho komunikace považována za podezřelou.

Optimální hodnota toho parametru závisí na konkrétních podmínkách (charakter činnosti uživatelů, typické síťové aplikace, které používají atd.) a je třeba ji najít experimentálně. Příliš nízká hodnota může způsobit nesprávný výsledek (tj. podezření na *P2P* síť u uživatele, který ji ve skutečnosti nepoužívá), naopak příliš vysoká hodnota zhoršuje úspěšnost detekce (nižší procento detekovaných *P2P* sítí).

„Bezpečné“ služby

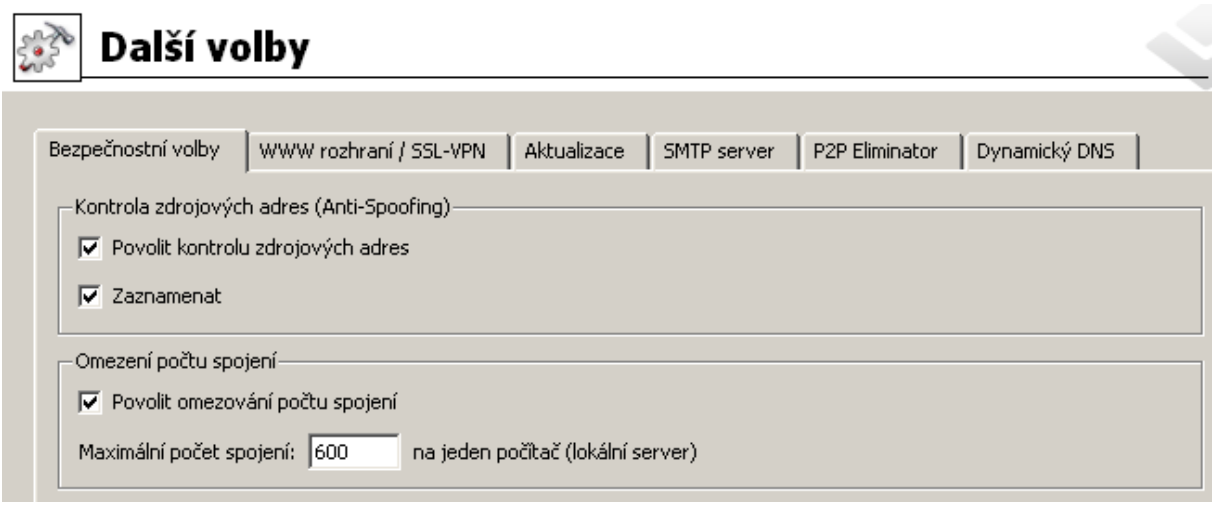
Určité legitimní služby mohou rovněž vykazovat charakteristiky komunikace v *P2P* sítích (např. velký počet současně otevřených spojení). Aby tato komunikace nebyla nesprávně detekována a uživatelé těchto služeb nebyli neprávem omezováni, je možné definovat seznam tzv. bezpečných služeb. Tyto služby budou vyloučeny z detekce *P2P* komunikace. Tlačítko *Definovat služby...* otevírá dialog pro nastavení služeb, které nebudou považovány za komunikaci v *P2P* síti. K dispozici všechny služby definované v sekci *Konfigurace* → *Definice* → *Služby* (podrobnosti viz kapitola 14.3).

Upozornění

Výchozí hodnoty parametrů detekce *P2P* sítí byly nastaveny empiricky na základě dlouhodobého testování. Jak již bylo uvedeno, v mnoha případech není možné s určitostí říci, zda daný uživatel skutečně používá *P2P* síť či nikoliv, a výsledkem je pouze určitá pravděpodobnost. Změna parametrů detekce může mít zásadní vliv na její výsledek. Z tohoto důvodu doporučujeme měnit parametry detekce *P2P* sítí pouze v opodstatněných případech (např. zjistíme nové číslo portu, které používá pouze *P2P* síť a žádná legitimní aplikace, nebo zjistíme, že určitá legitimní služba je opakovaně detekována jako *P2P* síť).

17.2 Volby pro zvýšení bezpečnosti

WinRoute nabízí několik bezpečnostních voleb, které nelze definovat komunikačními pravidly. Tyto volby lze aktivovat a nastavit v sekci *Konfigurace* → *Další volby*, záložka *Bezpečnostní volby*.



Obrázek 17.4 Bezpečnostní volby — Anti-Spoofing a omezení počtu spojení na jeden počítač

Kontrola zdrojových adres (Anti-Spoofing)

Anti-Spoofing je kontrola, zda na jednotlivá rozhraní počítače s *WinRoute* 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 k 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.

K nastavení funkce *Anti-Spoofing* slouží horní část záložky *Bezpečnostní volby*.

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 22.11).

Omezování počtu spojení

Tato bezpečnostní funkce umožňuje definovat maximální počet síťových spojení, která mohou být navázána z jednoho počítače (pracovní stanice) v lokální síti do Internetu nebo z Internetu na lokální server prostřednictvím mapovaného portu.

Příchozí a odchozí spojení jsou sledována odděleně. Pokud počet všech spojení navázaných z/na jeden lokální počítač v některém směru dosáhne nastavené hodnoty, *WinRoute* nepovolí otevřít další spojení v daném směru.

Uvedená omezení chrání firewall (počítač s *WinRoute*) proti přetížení a mohou zabránit útokům na cílový server, případně i zmírnit nežádoucí činnost červa či trojského koně.

Omezení počtu odchozích spojení se uplatní např. v případě, je-li klientský počítač v lokální síti je napaden červem nebo trojským koněm, který se snaží navázat spojení s velkým počtem různých serverů. Omezování počtu příchozích spojení může např. zabránit útoku *SYN flood* (zahlcení serveru současným navázáním velkého počtu spojení, kterými nejsou přenášena žádná data).

Kapitola 18

Další nastavení

18.1 Směrovací tabulka

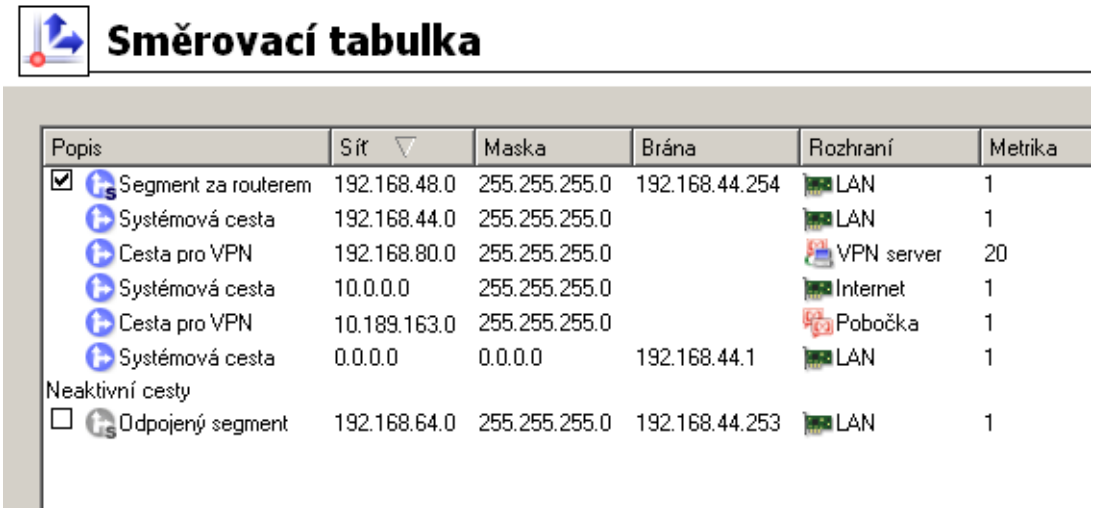
V programu *Administration Console* lze zobrazit a upravovat směrovací tabulku počítače, na němž je *WinRoute* nainstalován. Toto je velmi užitečné zejména při odstraňování problémů či úpravě konfigurace na dálku (není nutné používat aplikace pro terminálový přístup, sdílení pracovní plochy apod.).

K zobrazení a úpravě směrovací tabulky slouží sekce *Konfigurace* → *Směrovací tabulka*. Tato sekce zobrazuje aktuální směrovací tabulku operačního systému včetně tzv. trvalých tras (*persistent routes* — cesty přidané příkazem `route -p`).

Poznámka:

1. V režimu zálohování internetového připojení (viz kapitola 6.3) je vždy zobrazována pouze aktuální výchozí cesta (podle toho, které internetové rozhraní je právě aktivní).

2. V případě více internetových linek v režimu rozložení zátěže sítě (viz kapitola 6.4) bude zobrazena pouze jedna výchozí cesta, a to přes linku s nejvyšší deklarovanou rychlostí.



Obrázek 18.1 Zobrazení systémové směrovací tabulky firewallu

V sekci *Směrovací tabulka* je možné přidávat a rušit dynamické i statické cesty. Dynamická cesta je platná pouze do restartu operačního systému, případně do odstranění systémovým příkazem `route`. Statická cesta je cesta, kterou *WinRoute* trvale udržuje a obnoví ji i po restartu operačního systému.

Poznámka: Jestliže je *WinRoute* spravován vzdáleně, může změna ve směrovací tabulce způsobit přerušení spojení mezi *WinRoute Firewall Engine* a *Administration Console* (bezprostředně po stisknutí tlačítka *Použít*). Doporučujeme proto upravenou směrovací tabulku před stisknutím tlačítka *Použít* vždy důkladně zkontrolovat!

Typy cest

Ve směrovací tabulce ve *WinRoute* jsou rozlišovány tyto typy cest:

- *Systémové cesty* — cesty načtené ze směrovací tabulky operačního systému (včetně tzv. trvalých tras). Tyto cesty nelze měnit (některé z nich lze odebrat — viz sekce *Odstraňování cest ze směrovací tabulky*).
- *Statické cesty* — ručně definované cesty, které udržuje *WinRoute* (viz níže). Tyto cesty lze přidávat, měnit a odebírat dle potřeby.
  Zaškrtávací pole umožňuje cestu dočasně „vypnout“ — pak je zobrazována mezi neaktivními cestami. Statické cesty jsou označeny ikonou se symbolem *S*.
- *Cesty pro VPN* — cesty k VPN klientům a do sítí na vzdálených koncích VPN tunelů (podrobnosti viz kapitola 23). Tyto cesty jsou vytvářeny a rušeny dynamicky při připojování a odpojování VPN klientů nebo při vytváření a rušení VPN tunelů. Cesty pro VPN nelze ručně vytvářet, měnit ani odebírat.
- *Neaktivní cesty* — cesty, které jsou v daném okamžiku neaktivní, se zobrazují odděleně. Neaktivní cesty mohou být např. „vypnuté“ statické cesty, statické cesty přes rozhraní, které bylo odpojeno nebo odebráno ze systému apod.

Statické cesty

WinRoute obsahuje speciální mechanismus pro vytváření a udržování statických cest ve směrovací tabulce. Veškeré statické cesty definované ve *WinRoute* 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“ — je-li některá z nich odstraněna příkazem `route`, *WinRoute* ji okamžitě opět přidá.

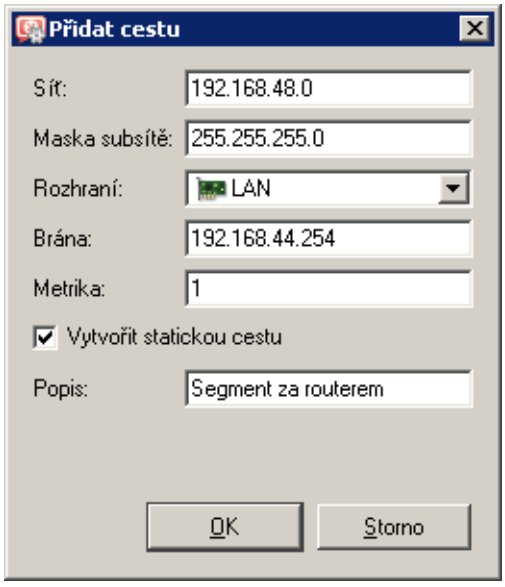
Poznámka:

1. K implementaci statických cest nejsou využívány trvalé trasy operačního systému (*WinRoute* používá vlastní metodu udržování těchto cest).

2. Vede-li statická cesta přes vytáčené rozhraní (telefonické připojení), pak UDP paket nebo TCP paket s příznakem *SYN* směrovaný touto cestou způsobí vytočení linky. Podrobné informace viz kapitola 6.2.

Definice dynamických a statických cest

Po stisknutí tlačítka *Přidat* (resp. *Změnit* na vybrané cestě) se zobrazí dialog pro definici cesty.



Obrázek 18.2 Přidání cesty do směrovací tabulky

Síť, Maska subsítě
: 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.

Vytvořit statickou cestu
: Při zaškrtnutí této volby bude cesta označena jako statická, tzn. *WinRoute* ji bude automaticky obnovovat (viz výše). Do pole *Popis* je vhodné uvést stručnou charakteristiku přidávané cesty (proč byla přidána, do jaké sítě vede apod.).
Neoznačíme-li cestu jako statickou, pak bude platná pouze do vypnutí počítače nebo do ručního odstranění (příkazem `route` nebo v *Administration Console*).

Odstraňování cest ze směrovací tabulky

Pomocí administrační konzole *WinRoute* lze záznamy ze směrovací tabulky také mazat (tlačítkem *Odebrat*). Pro mazání cest platí následující pravidla:

- Statické cesty jsou plně v režii *WinRoute*. Zrušení statické cesty znamená její okamžité a trvalé odebrání ze systémové směrovací tabulky (po stisknutí tlačítka *Použít*).
- Dynamická (systémová) cesta bude rovněž trvale odstraněna. Nezáleží na tom, zda byla přidána pomocí *Administration Console* nebo příkazem `route`. Nelze však odstranit cestu do sítě přímo připojené k některému rozhraní.
- Trvalá trasa operačního systému 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 trvalé trasy 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 trvalá trasa vytvořena a jak ji trvale zrušit.

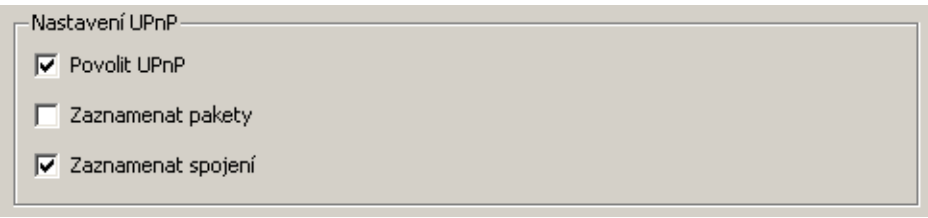
18.2 Universal Plug-and-Play (UPnP)

WinRoute obsahuje podporu protokolu UPnP (*Universal Plug-and-Play*). Tento protokol umožňuje klientské aplikaci (např. *Microsoft MSN Messenger*) detekovat firewall a vyžádat si otevření (mapování) potřebných portů z Internetu na příslušný počítač v lokální síti. Toto mapování je vždy pouze dočasné — platí buď do uvolnění portů samotnou aplikací (pomocí zpráv protokolu UPnP) nebo do vypršení určitého časového limitu.

Požadovaný port nesmí kolidovat s žádným existujícím mapovaným portem a s žádným komunikačním pravidlem povolujícím přístup z Internetu na firewall. Při nesplnění těchto podmínek bude UPnP požadavek na mapování portu zamítnut.

Konfigurace podpory protokolu UPnP

Konfigurace UPnP se provádí v sekci *Konfigurace* → *Další volby*, záložka *Bezpečnostní volby*.



Obrázek 18.3 Nastavení podpory UPnP (sekce Konfigurace → Další volby, záložka Bezpečnostní volby)

Povolit UPnP

Zapnutí funkce *UPnP*.

Upozornění

Je-li *WinRoute* provozován na operačním systému *Windows XP*, *Windows Server 2003*, *Windows Vista* nebo *Windows Server 2008*, pak se před zapnutím funkce *UPnP* přesvědčte, že nejsou spuštěny tyto systémové služby:

- *Služba rozpoznávání pomocí protokolu SSDP (SSDP Discovery Service)*
- *Hostitel zařízení UPnP (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*.

Poznámka: Instalační program *WinRoute* uvedené služby detekuje a nabízí jejich zastavení a zakázání.

Zaznamenat pakety

Po zapnutí této volby budou do záznamu *Filter* (viz kapitola 22.9) zaznamenány všechny pakety procházející přes porty mapované pomocí UPnP.

Zaznamenat spojení

Po zapnutí této volby budou do záznamu *Connection* (viz kapitola 22.5) 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 7.3) 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	UPnP klienti	Libovolný	UPnP	✓
Zákaz UPnP	Důvěryhodné / lokální	Libovolný	UPnP	✗

Obrázek 18.4 Komunikační pravidla pro povolení UPnP vybraným počítačům

První pravidlo povolí používání UPnP pouze ze skupiny IP adres *Klienti UPnP*. Druhé pravidlo zakáže používání UPnP ze všech ostatních počítačů (IP adres).

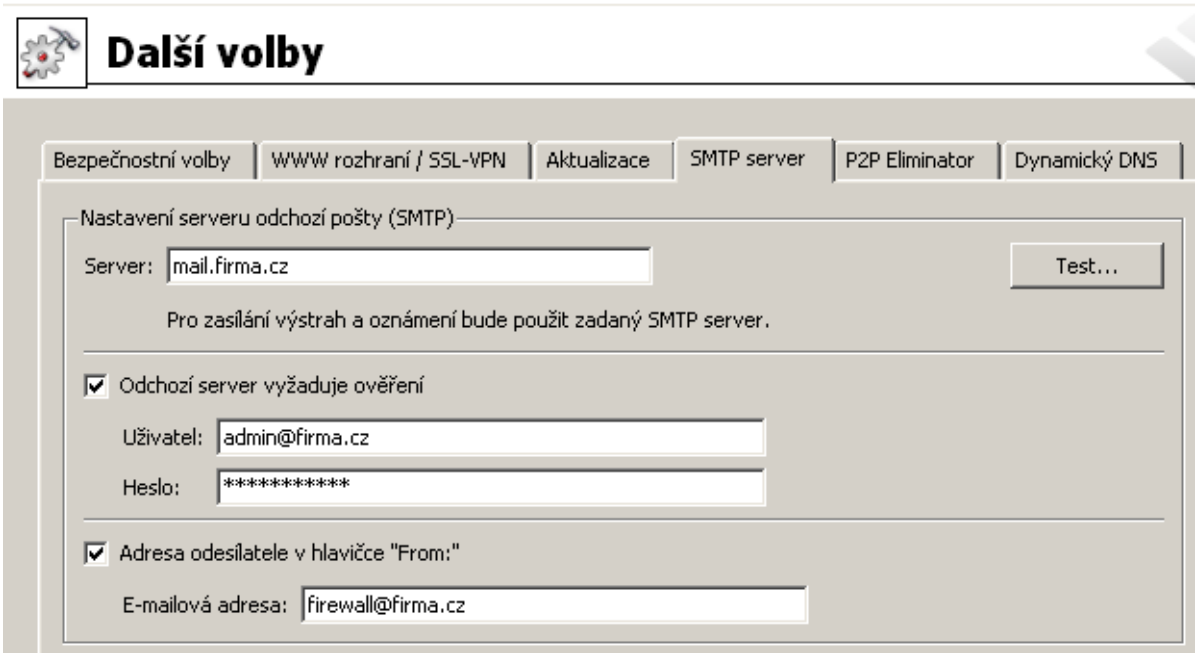
18.3 Nastavení serveru odchozí pošty

WinRoute může při určitých událostech posílat uživatelům, resp. správcům, informativní nebo varovné e-mailové zprávy. E-mail může být odeslán např. při zachycení viru (viz kapitola 13.3), při detekci *Peer-to-Peer* sítě (viz kapitola 17.1), při překročení kvóty objemu přenesených dat (viz kapitola 15.1) nebo na základě nastavených výstrah (viz kapitola 19.4).

Pro odeslání e-mailu musí mít *WinRoute* k dispozici SMTP server (podobně jako poštovní klient vyžaduje nastavení serveru odchozí pošty). Tento server se používá také při antivirové kontrole e-mailů pro přeposílání zpráv obsahujících viry na zadanou adresu.

Poznámka: WinRoute neobsahuje žádný vlastní (vestavěný) SMTP server.

Server pro odesílání e-mailových zpráv lze nastavit v sekci *Konfigurace* → *Další volby*, záložka *SMTP server*.



Obrázek 18.5 Nastavení SMTP serveru pro odesílání informativních a varovných zpráv

Server

Jméno nebo IP adresa SMTP serveru, který má být použit.

Je-li to možné, doporučujeme použít SMTP server v lokální síti (většina zpráv, které *WinRoute* odesílá, je zpravidla určena lokálním uživatelům).

Odchozí server vyžaduje ověření

Tuto volbu je třeba zapnout v případě, kdy SMTP server nastavený v položce *Server* vyžaduje ověření uživatele jménem a heslem.

Adresa odesílatele v hlavičce From

Tato volba umožňuje nastavit e-mailovou adresu odesílatele (tj. hodnotu položky `From` v hlavičce zprávy) ve zprávách odeslaných *WinRoute* (výstrahy zasílané uživatelům for-

mou e-mailů nebo krátkých textových zpráv). Nastavení odchozí adresy nemá vliv na zprávy přeposílané při antivirové kontrole (viz kapitola 13.4).
E-mailovou adresu pro hlavičku `From` je třeba nastavit zejména v případě, pokud použitý SMTP server provádí striktní kontrolu této hlavičky (zprávy bez hlavičky `From` nebo s neplatnou adresou v této hlavičce jsou považovány za spam). I v případech, kdy není vyžadována SMTP serverem, může adresa odesílatele sloužit k třídění zpráv nebo pro zvýšení přehlednosti v poštovním klientovi příjemce. Z tohoto důvodu doporučujeme e-mailovou adresu odesílatele ve *WinRoute* vždy zadávat.

Test

Tlačítkem *Test* lze ověřit funkčnost odesílání e-mailových zpráv přes zadaný SMTP server. *WinRoute* pošle zkušební zprávu na zadanou e-mailovou adresu.

Upozornění

1. Je-li SMTP server zadán DNS jménem, může být používán až od okamžiku, kdy *WinRoute* zjistí odpovídající IP adresu (DNS dotazem). Dokud není IP adresa známa, zobrazuje se v záložce *SMTP server* varování *Nelze zjistit IP adresu zadaného SMTP serveru*. Po úspěšném zjištění příslušné IP adresy z DNS (zpravidla do několika sekund) varování zmizí.

   Zůstává-li varování v záložce *SMTP server* zobrazeno, znamená to, že je buď zadáno chybné (neexistující) DNS jméno nebo nastala komunikační chyba (DNS server neodpovídá). Je-li to možné, doporučujeme zadávat SMTP server IP adresou.

2. Komunikace s SMTP serverem nesmí být blokována komunikačními pravidly, jinak se po stisknutí tlačítka *Použít* zobrazí chybové hlášení *Spojení na SMTP server je blokováno komunikačními pravidly*.

   Podrobné informace o komunikačních pravidlech naleznete v kapitole 7.

Kapitola 19

Stavové informace

WinRoute umožňuje správci (popř. jinému oprávněnému uživateli) poměrně detailně sledovat činnost firewallu. V podstatě se jedná o tři druhy informací: sledování stavu, statistiky a záznamy.

- Sledovat lze komunikaci jednotlivých počítačů, přihlášené uživatele a spojení, která jsou přes *WinRoute* navázána.
  Poznámka:
  1. *WinRoute* sleduje pouze komunikaci mezi lokální sítí a Internetem. Komunikace v rámci lokální sítě není sledována.
  2. Zobrazuje se pouze komunikace, která je povolena komunikačními pravidly (viz kapitola 7). Pokud je zobrazena komunikace, o níž se domníváte, že by měla být zakázána, je třeba hledat chybu v nastavení pravidel.
- Statistiky obsahují informace o uživatelích a síťové komunikaci za určité časové období. Statistiky jsou zobrazovány v podobě tabulek nebo grafů. Podrobnosti viz kapitola 20.
- 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*). Podrobnosti naleznete v kapitole 22.

Jaké informace lze sledovat a jak lze přizpůsobit sledování potřebám uživatele je popsáno v následujících kapitolách.

19.1 Aktivní počítače a přihlášení uživatelé

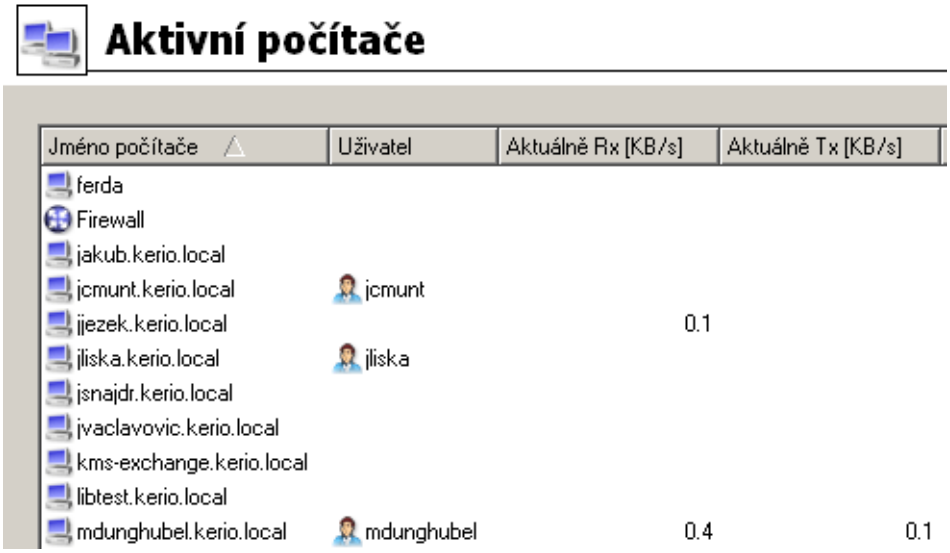
V sekci *Stav* → *Aktivní počítače* se zobrazují počítače z lokální sítě, případně přihlášení uživatelé, kteří komunikují přes *WinRoute* do Internetu.

Poznámka: Podrobnosti o přihlašování uživatelů na firewall naleznete v kapitole 10.1.

V horní části okna jsou zobrazeny jednotlivé počítače a informace o přihlášených uživatelích, objemu a rychlosti přenášených dat atd.

V okně *Aktivní počítače* mohou být zobrazeny následující informace:

Jméno počítače
: DNS jméno počítače. Není-li nalezen odpovídající DNS záznam, zobrazuje se namísto jména počítače IP adresa.



Obrázek 19.1 Přehled aktivních počítačů a uživatelů přihlášených na firewall

Uživatel
Jméno uživatele, který je z daného počítače přihlášen. Není-li přihlášen žádný uživatel, je tato položka prázdná.

Aktuálně Rx, Aktuálně Tx
Aktuální přenosová rychlost (v kilobytech za sekundu) v každém směru (*Rx* = příchozí data, *Tx* = odchozí data) z pohledu daného počítače.

Následující sloupce jsou ve výchozím nastavení skryty. Pro jejich zobrazení použijte volbu *Nastavit sloupce* z kontextového menu (viz níže).

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 11.1).

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*.

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 proxy server ve *WinRoute*, na němž se ověřil,
- *NTLM* — uživatel byl automaticky ověřen v NT doméně pomocí NTLM (funguje při použití prohlížeče *Internet Explorer* verze 5.5 a vyšší nebo *Firefox/SeaMonkey* verze jádra 1.3 a vyšší),
- *VPN klient* — uživatel se připojil do lokální sítě pomocí aplikace *Kerio VPN Client* (podrobnosti viz kapitola 23).
  Poznámka: Pro VPN klienty se nezobrazují spojení a neměří se objem přenesených dat.

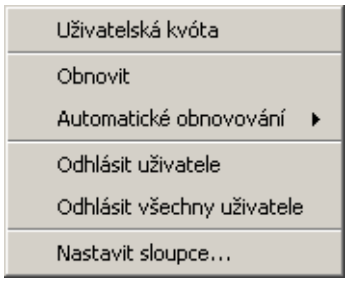
Detaily o přihlašování a ověřování uživatelů naleznete v kapitole 10.1.

Tlačítko *Obnovit* slouží k obnovení informací zobrazených v okně *Aktivní počítače*.

Tlačítko *Zobrazit / Skrýt podrobnosti* otevírá, resp. zavírá dolní část okna s detailními informacemi o uživateli, počítači a otevřených spojení.

Volby pro okno Aktivní počítače

Stisknutím pravého tlačítka myši v okně *Aktivní počítače* (resp. přímo na vybraném záznamu) se zobrazí kontextové menu s následujícími volbami:



Obrázek 19.2 Kontextové menu okna Aktivní počítače

Uživatelská kvóta
Tato volba zobrazí informace o kvótě příslušného uživatele (*Administration Console* se přepne do sekce *Stav* → *Statistiky*, záložka *Uživatelská kvóta* a automaticky vybere příslušného uživatele).
Volba *Uživatelská kvóta* je v kontextovém menu dostupná pouze pro počítače, z nichž je k firewallu přihlášen některý uživatel.

Obnovit
Okamžité obnovení informací v okně *Aktivní počítače* (tato funkce je identická s funkcí tlačítka *Obnovit* pod oknem).

Automatické obnovování
Nastavení automatického obnovování informací v okně *Aktivní počítače*. Informace mohou být automaticky obnovovány v intervalu 5 sekund až 1 minuta nebo je možné automatické obnovování vypnout (*Neobnovovat*).

Odhlásit uživatele
Okamžité odhlášení vybraného uživatele od firewallu.

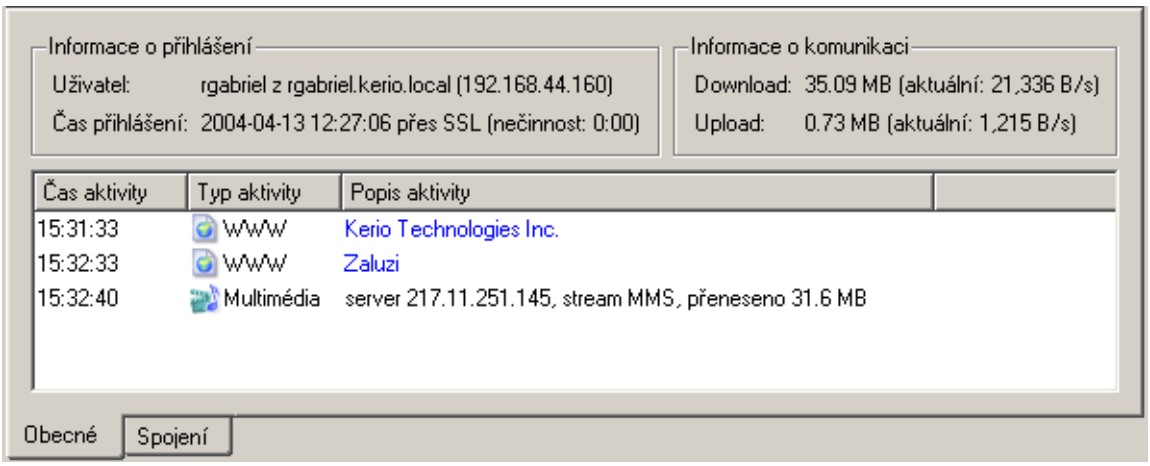
Odhlásit všechny uživatele
Okamžité odhlášení všech přihlášených uživatelů od firewallu.

Nastavit sloupce
Volba sloupců, která mají být v okně *Aktivní počítače* zobrazeny (podrobnosti viz kapitola 3.2).

Podrobné informace o vybraném počítači a uživateli

V dolní části sekce *Aktivní počítače* se zobrazují detailní informace o vybraném počítači, příp. přihlášeném uživateli.

Záložka *Obecné* obsahuje informace o přihlášení uživatele, objemu a rychlosti přenášených dat a rozpoznaných aktivitách uživatele.



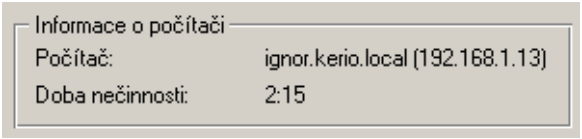
Obrázek 19.3 Informace o vybraném počítači a uživateli — přehled aktivit

Přihlašovací údaje

Informace o přihlášeném uživateli:

- *Uživatel* — jméno uživatele, DNS jméno (je-li k dispozici) a IP adresa počítače, ze kterého je přihlášen
- *Čas přihlášení* — datum a čas přihlášení uživatele, použitá ověřovací metoda a doba nečinnosti

Není-li z daného počítače přihlášen žádný uživatel, zobrazují se namísto přihlašovacích údajů podrobnosti o tomto počítači.



Obrázek 19.4 Informace o počítači (není-li z něj přihlášen žádný uživatel)

- *Počítač* — DNS jméno (je-li k dispozici) a IP adresa počítače
- *Doba nečinnosti* — doba, po kterou nebyla detekována žádná síťová aktivita tohoto počítače

Informace o komunikaci

Objem dat přijatých (*Download*) a vyslaných (*Upload*) daným uživatelem (resp. z daného počítače) a aktuální přenosová rychlost v každém směru.

V hlavním poli záložky *Obecné* se zobrazuje seznam zjištěných aktivit daného uživatele (resp. počítače):

Čas aktivity

Čas (s přesností na sekundy), kdy byla aktivita zachycena.

Typ aktivity

Typ detekované aktivity (síťové komunikace). *WinRoute* rozpoznává tyto aktivity: *SMTP*, *POP3*, *WWW* (komunikace protokolem HTTP), *FTP*, *Multimédia* (přenos obrazu a zvuku v reálném čase) a *P2P* (používání Peer-to-Peer sítí).

Poznámka: WinRoute nerozpoznává konkrétní *P2P* síť, pouze na základě určitých testů vyhodnotí, že klient je pravděpodobně do takové sítě připojen. Podrobnosti naleznete v kapitole 17.1.

Popis aktivity

Detailní informace o příslušné aktivitě:

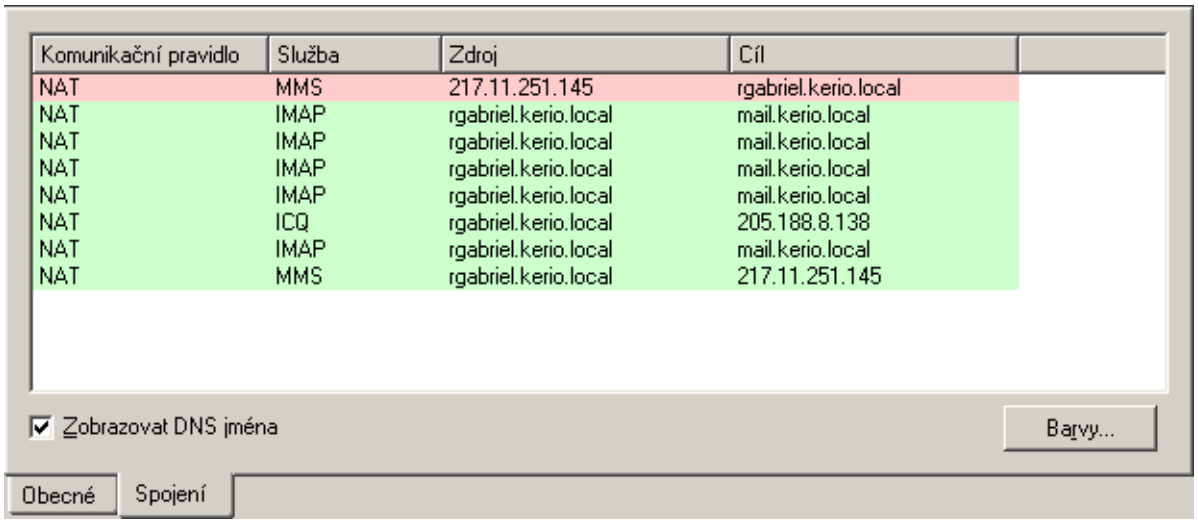
- *WWW* — titulek WWW stránky, na kterou uživatel přistupuje (nemá-li stránka titulek, zobrazí se její URL). Titulek stránky je hypertextový odkaz — po kliknutí se ve WWW prohlížeči, který je v operačním systému nastaven jako výchozí, zobrazí příslušná stránka.

  Poznámka: Z důvodu přehlednosti se zde zobrazuje pouze první navštívená stránka z každého WWW serveru, na který uživatel navštívil. Podrobné informace o všech navštívených stránkách jsou k dispozici v *Kerio StaR* (viz kapitola 21).
- *SMTP, POP3* — DNS jméno nebo IP adresa serveru, objem přijatých a vyslaných dat.

- *FTP* — DNS jméno nebo IP adresa serveru, objem stažených a uložených dat, informace o aktuálně stahovaném nebo ukládaném souboru (jméno souboru včetně cesty, objem přijatých nebo odeslaných dat z tohoto souboru).
- *Multimédia* (přenos videa a zvuku v reálném čase) — DNS jméno nebo IP adresa serveru, použitý protokol (*MMS*, *RTSP*, *RealAudio* atd.) a objem stažených dat.
- *P2P* — informace o tom, že klient pravděpodobně používá Peer-To-Peer síť.

Informace o spojeních z/do Internetu

Záložka *Spojení* zobrazuje detailní informace o spojeních navázaných z vybraného počítače do Internetu nebo z Internetu na tento počítač (např. prostřednictvím mapovaných portů, *UPnP* apod.). Výpis spojení dává podrobný přehled o tom, jaké služby příslušný uživatel využívá. Nežádoucí spojení je možné okamžitě ukončit.



Obrázek 19.5 Informace o vybraném počítači a uživateli — přehled spojení

Zobrazované informace o spojení:

Komunikační pravidlo
: Název komunikačního pravidla *WinRoute* (viz kapitola 7), kterým bylo příslušné spojení povoleno.

Služba
: Název (zkratka) aplikační služby. Pokud se nejedná o standardní službu, zobrazuje se číslo portu a protokol.

Zdroj, Cíl
: Zdrojová a cílová IP adresa (příp. jméno počítače, je-li zapnuta volba *Zobrazovat DNS jména* — viz níže).

Následující informace jsou ve výchozím nastavení skryty. Jejich zobrazení je možné nastavit volbou *Nastavit sloupce* z kontextového menu (podrobnosti viz kapitola 3.2).

Zdrojový port, Cílový port
: Zdrojový a cílový port (pouze v případě transportních protokolů TCP a UDP).

Protokol
: Použitý transportní protokol (TCP, UDP atd.).

Časový limit
: Doba zbývající do odstranění spojení z tabulky spojení *WinRoute*.
S každým novým paketem v rámci tohoto spojení je časový limit nastaven na výchozí hodnotu. Nejsou-li spojením přenášena žádná data, *WinRoute* jej po uplynutí časového limitu vymaže z tabulky — tím se spojení de facto uzavře a nelze jím přenášet žádná další data.

Rx, Tx
: Objem dat přijatých (*Rx*) a vyslaných (Tx) tímto spojením (v kilobytech).

Informace
: Upřesňující informace (např. v případě protokolu HTTP metoda a URL požadavku).

Volba *Zobrazovat DNS jména* zapíná/vypíná zobrazení DNS jmen počítačů namísto IP adres v položkách *Zdroj* a *Cíl*. Nepodaří-li se DNS jméno pro určitou IP adresu zjistit, zůstává na příslušném místě zobrazena IP adresa.

Tlačítko *Barvy* otevírá dialog pro nastavení barev pro zobrazení spojení.

Poznámka:

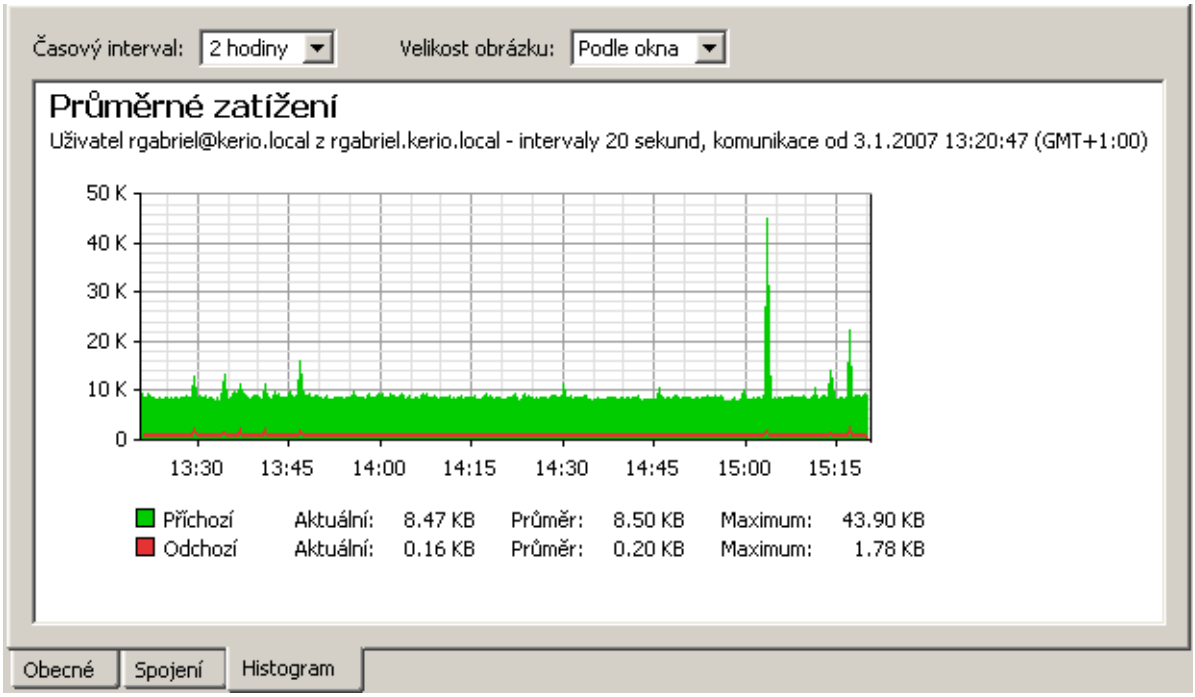
1. Při kliknutí pravým tlačítkem myši na určitém spojení je výše popsané kontextové menu rozšířeno o položku *Ukončit spojení* — touto volbou lze okamžitě ukončit nežádoucí spojení navázané mezi lokální sítí a Internetem.

2. V přehledu spojení pro daný počítač jsou zobrazována pouze spojení navázaná z tohoto počítače do Internetu nebo z Internetu na tento počítač. Lokální spojení navázaná mezi daným počítačem a firewallem lze zobrazit pouze v sekci *Stav* → *Spojení* (viz kapitola 19.2). Spojení mezi počítači v lokální síti *WinRoute* nezachytí, a proto je nelze zobrazit.

Časový průběh zatížení linky

Záložka *Histogram* zobrazuje časový průběh objemu přenesených dat pro vybraný počítač. Graf dává přehled o tom, jak daný počítač zatěžuje internetovou linku v průběhu dne.

V položce *Časový interval* lze vybrat časové období, pro které bude graf zobrazen (2 hodiny nebo 1 den). Vodorovná osa grafu představuje čas a svislá osa rychlost přenosu. Měřítko vodorovné osy je určeno vybraným časovým obdobím a měřítko svislé osy je nastavováno automaticky podle maximální hodnoty ve sledovaném období (základní jednotkou jsou byty — *B*).



Obrázek 19.6 Informace o vybraném počítači a uživateli — časový průběh zatížení linky

Pro tento graf se vyhodnocuje objem přenesených dat v daném směru v určitých časových intervalech (v závislosti na zvoleném období). Zelená křivka zobrazuje průběh objemu přenesených dat v příchozím směru (download) ve vybraném časovém období, plocha pod křivkou vyjadřuje celkový objem přenesených dat za toto období. Červená křivka a plocha dávají tytéž informace pro data v odchozím směru (upload). Pod grafem jsou dále zobrazeny základní statistické informace — aktuální objem přenesených dat (v posledním intervalu) a průměrný a maximální objem dat v jednom intervalu.

Volba *Velikost obrázku* umožňuje nastavit pevnou velikost grafu nebo přizpůsobit jeho velikost oknu *Administration Console*.

19.2 Zobrazení síťových 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

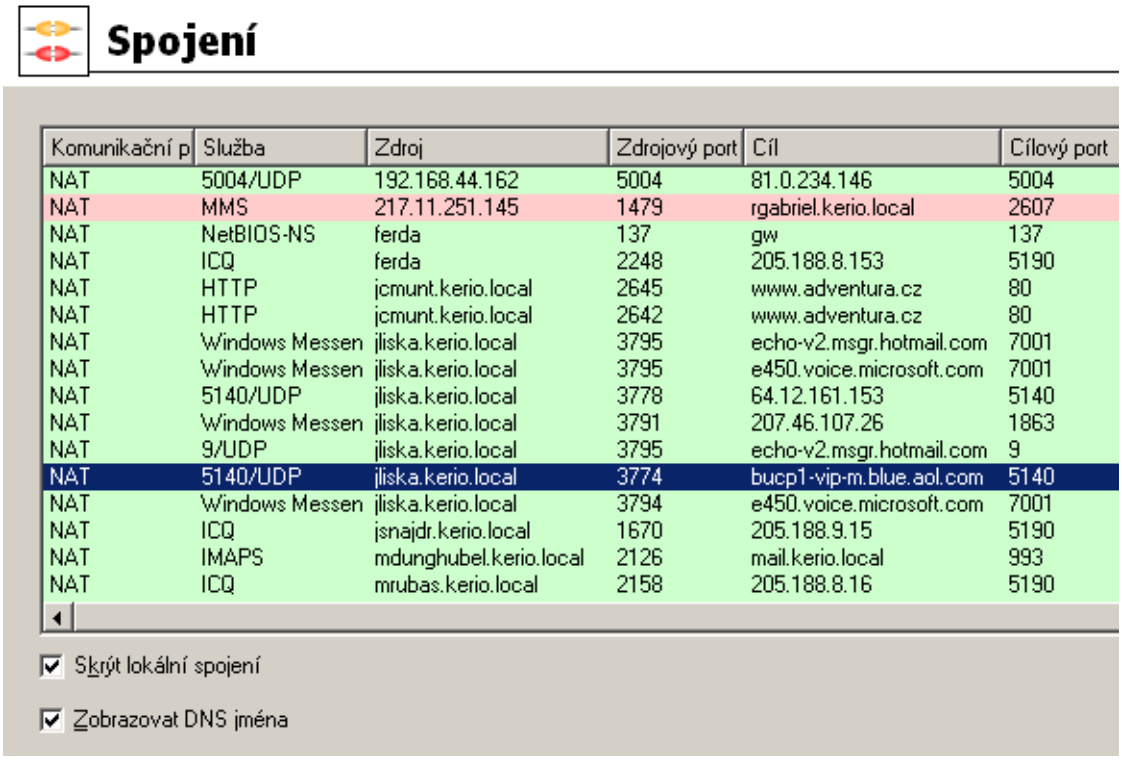
Správce *WinRoute* může vybrané spojení „násilně“ ukončit.

Poznámka:

1. *WinRoute* nezachytí (a tudíž nezobrazí) spojení navázaná mezi lokálními klienty.

2. Protokol UDP je tzv. nespojovaný protokol — nenavazuje žádné spojení, komunikace pro-

bíhá formou jednotlivých zpráv (tzv. datagramů). V tomto případě jsou sledována tzv. pseudospojení (periodická výměna zpráv mezi dvěma počítači je považována za jedno spojení).



Obrázek 19.7 Přehled všech spojení navázaných přes WinRoute

Na každé řádce okna *Spojení* je zobrazeno jedno spojení. Jedná se o síťová spojení, nikoliv připojení uživatelů — každý klientský program může navázat více spojení současně (např. z důvodu rychlejší komunikace).

Sloupce zobrazují následující informace:

Komunikační pravidlo
: Název komunikačního pravidla, kterým bylo povoleno navázání příslušného spojení (viz kapitola 7).

Služba
: Název služby, která je tímto spojením přenášena (je-li taková služba ve *WinRoute* definována — viz kapitola 14.3). Pokud *WinRoute* danou službu nezná, zobrazí se číslo portu a protokol (např. *5004/UDP*).

Zdroj, Cíl
: IP adresa zdroje (iniciátora spojení) a cíle. Pokud existuje v DNS příslušný reverzní záznam, zobrazuje se místo IP adresy odpovídající DNS jméno.

Následující sloupce jsou ve výchozím nastavení skryty. Pro jejich zobrazení použijte volbu *Nastavit sloupce* v kontextovém menu (viz kapitola 3.2).

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.

Info
Textová informace o daném spojení (např. inspekční modul, který byl na toto spojení aplikován).

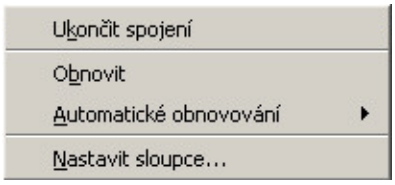
Informace v okně *Spojení* jsou automaticky obnovovány v nastaveném intervalu, navíc je také lze obnovit ručně tlačítkem *Obnovit*.

Volby pro okno Spojení

Pod seznamem spojení se nacházejí tyto volby:

- *Skrýt lokální spojení* — v okně *Spojení* nebudou zobrazena spojení navázaná z a/nebo na počítač s *WinRoute*.
  Tuto volbu lze využít pro zvýšení přehlednosti (pokud nás zajímají pouze spojení počítačů v lokální síti).
- *Zobrazovat DNS jména* — tato volba zapíná zobrazení DNS jmen počítačů namísto IP adres. Pokud pro určitou IP adresu neexistuje odpovídající DNS záznam (příp. do doby, než je zjištěno odpovídající jméno), zůstává zobrazena IP adresa.

Stisknutím pravého tlačítka myši v okně *Spojení*, resp. přímo na vybraném spojení, se zobrazí kontextové menu s následujícími volbami:



Obrázek 19.8 Kontextové menu okna Spojení

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.

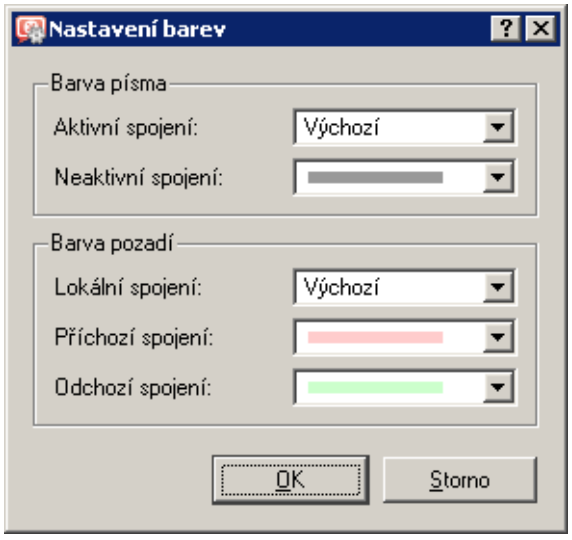
Obnovit
Okamžité obnovení informací v okně *Spojení* (tato funkce je identická s funkcí tlačítka *Obnovit* v dolní části okna).

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 3.2).

Nastavení barev

Tlačítko *Barvy* slouží k nastavení barev, kterými budou jednotlivá spojení zobrazována:



Obrázek 19.9 Nastavení barev pro zobrazování spojení

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)

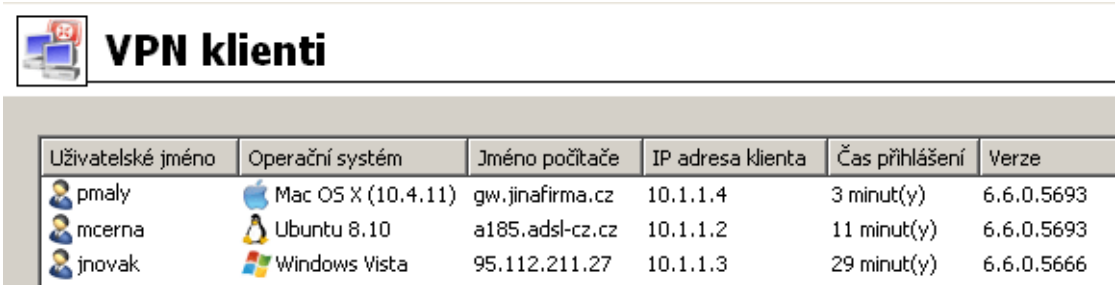
Barva pozadí

- *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 7.

19.3 Přehled připojených VPN klientů

V sekci *Stav* → *VPN klienti* lze získat přehled o VPN klientech aktuálně připojených k VPN serveru ve *WinRoute*.



Obrázek 19.10 Přehled připojených VPN klientů

O připojených klientech jsou zobrazeny tyto informace:

- Uživatelské jméno, kterým se klient přihlásil k firewallu. VPN komunikace bude zahrnuta do statistik tohoto uživatele.
- Operační systém, na kterém má příslušný uživatel nainstalovanou aplikaci *Kerio VPN Client*.
- DNS jméno počítače, ze kterého se klient přihlašuje. Pokud *WinRoute* nedokáže zjistit z DNS odpovídající jméno počítače, zobrazí se jeho (veřejná) IP adresa.
- IP adresa přidělená klientovi VPN serverem. Pod touto IP adresou klient „vystupuje“ v lokální síti.
- Doba, po kterou je klient přihlášen.
- Verze aplikace *Kerio VPN Client*, včetně čísla sestavení (buildu).

Následující dva sloupce jsou ve výchozím nastavení okna *VPN klienti* skryté (nastavení zobrazovaných sloupců viz kapitola 3.2):

- IP adresa — veřejná IP adresa počítače, ze kterého se klient připojuje (viz výše — sloupec *Jméno počítače*).
- Stav klienta — *připojuje se*, *ověřuje se* (*WinRoute* kontroluje uživatelské jméno a heslo), *ověřen* (jméno a heslo je správné, probíhá konfigurace klienta), *připojen* (konfigurace je dokončena, klient může komunikovat s počítači v lokální síti).

Poznámka: Odpojení klienti jsou ze seznamu automaticky odebráni.

19.4 Výstrahy

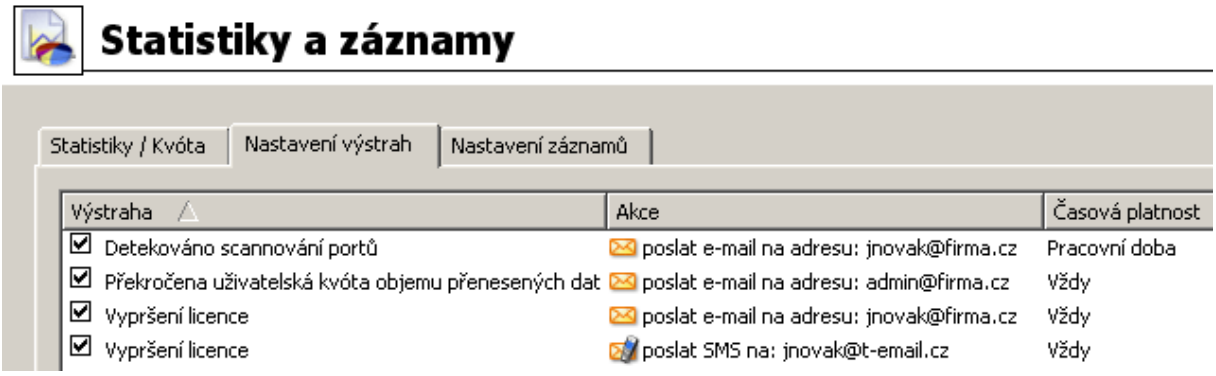
WinRoute může automaticky informovat správce o důležitých událostech, které zpracovával nebo zachytil. Díky tomuto mechanismu není nutné se k *WinRoute* pravidelně přihlašovat pomocí *Administration Console* a kontrolovat všechny stavové informace a záznamy (občasná kontrola však rozhodně není na škodu!).

WinRoute generuje výstrahu vždy při zachycení některé ze sledovaných událostí. Všechny tyto výstrahy se zapisují do záznamu *Alert* (viz kapitola 22.3). Správce *WinRoute* může nastavit, které z těchto výstrah mají být zasílány, komu a v jakém formátu. Odeslané výstrahy lze zároveň přehledně sledovat v sekci *Stav* → *Výstrahy*.

Poznámka: Pro odesílání výstrah musí být ve *WinRoute* nastaven server odchozí pošty (viz kapitola 18.3).

Nastavení výstrah

Zasílání výstrah na vybrané události lze nastavit v sekci *Konfigurace* → *Statistiky a záznamy*, záložka *Nastavení výstrah*.



Obrázek 19.11 Výstrahy ve WinRoute

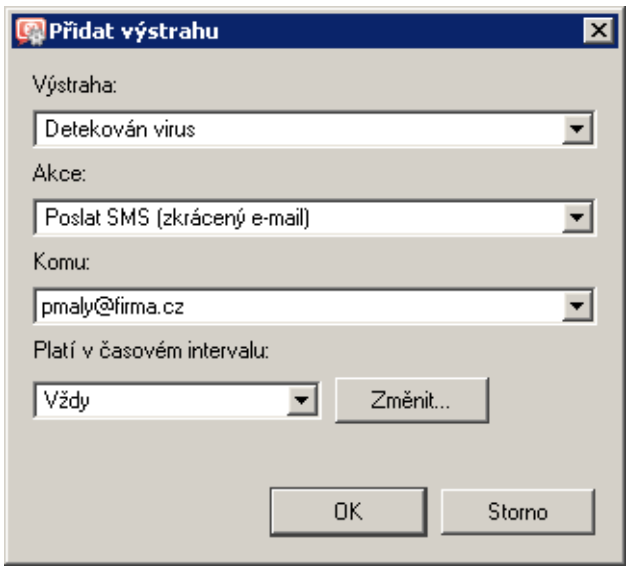
Tato záložka obsahuje seznam „pravidel“ pro zasílání výstrah. Zaškrtávací pole vlevo vedle každého pravidla slouží k jeho aktivaci/deaktivaci (např. pro dočasné vypnutí zasílání určité výstrahy).

Tlačítko *Přidat*, resp. *Změnit* otevírá dialog pro definici pravidla pro zasílání výstrahy.

Výstraha

Typ události, při které bude tato výstraha zasílána:

- *Detekován virus* — antivirový program nalezl virus v souboru přenášeném protokolem HTTP, FTP, SMTP nebo POP3 (viz kapitola 13).
- *Detekováno scannování portů* — *WinRoute* zachytil útok typu *port scanning* (buď na počítač, na kterém je nainstalován, nebo procházející).



Obrázek 19.12 Definice výstrahy

- *Dosaženo limitu počtu spojení na jeden počítač* — některý počítač v lokální síti má otevřen maximální povolený počet spojení (viz kapitola 17.2). Tento stav může indikovat přítomnost nežádoucí síťové aplikace (např. trojského koně nebo spyware) na příslušném počítači.
- *Nedostatek místa na disku* — varování, že na disku, kde je *WinRoute* nainstalován, zbývá již velmi málo místa (méně než 11% kapacity disku).
  WinRoute potřebuje diskový prostor pro ukládání záznamů, statistik, konfigurace, dočasných souborů (např. stažený instalační archiv nové verze nebo soubor, který je právě kontrolován antivirovým programem) a dalších informací. Obdrží-li správce *WinRoute* toto upozornění, měl by neprodleně provést příslušná opatření (uvolnění místa na disku, výměna disku za větší apod.)
- *Nová verze WinRoute ke stažení* — modul automatické kontroly nových verzí nalezl na serveru firmy Kerio Technologies novější verzi *WinRoute*. Správce může tuto verzi stáhnout a nainstalovat pomocí *Administration Console* (viz kapitola 16.3), případně z WWW stránek `http://www.kerio.cz/`.
- *Překročena uživatelská kvóta objemu přenesených dat* — některý uživatel překročil nastavený denní, týdenní nebo měsíční limit objemu přenesených dat a *WinRoute* provedl příslušnou akci. Podrobnosti viz kapitola 15.1.
- *Přepnutí primárního/záložního internetového připojení* — došlo k výpadku internetového připojení a přepnutí na záložní linku nebo naopak přepnutí zpět na primární linku. Podrobné informace naleznete v kapitole 6.3.
- *Vypršení licence* — blíží se datum skončení platnosti licence nebo předplatného *WinRoute* nebo některého z integrovaných modulů (*Kerio Web Filter*, antivirus *McAfee*). Správce *WinRoute* by měl zkontrolovat data vypršení a obnovit příslušnou licenci nebo předplatné (podrobnosti viz kapitola 4).
- *Vytočení / zavěšení RAS linky* — *WinRoute* vytáčí, resp. zavěšuje některou z RAS linek (viz kapitola 5). Upozornění obsahuje podrobné informace o této události:

jméno linky, důvod vytočení, jméno uživatele a IP adresu počítače, ze kterého byl požadavek přijat.

Akce

Způsob informování uživatele:

- *Poslat e-mail* — zaslání standardní e-mailové zprávy.
- *Poslat SMS (zkrácený e-mail)* — zaslání krátké textové zprávy (SMS) na mobilní telefon.
  Poznámka: SMS je rovněž zasílána formou e-mailu. Uživatel mobilního telefonu musí mít zřízenu odpovídající e-mailovou adresu (např. `cislo@operator.cz`). Zasílání SMS přímo na telefonní číslo (např. přes GSM bránu připojenou k počítači s *WinRoute*) není podporováno.

Komu

E-mailová adresa příjemce zprávy, resp. příslušného mobilního telefonu (závisí na volbě v položce *Akce*).
V položce *Komu* lze vybírat ze seznamu e-mailových adres použitých v ostatních výstrahách, případně zadat novou e-mailovou adresu.

Platí v časovém intervalu

Výběr časového intervalu, ve kterém bude výstraha uživateli zasílána. Tlačítkem *Změnit* lze časový interval upravit, případně vytvořit nový (podrobnosti viz kapitola 14.2).

Šablony výstrah

Formát zpráv zasílaných uživatelům (e-mailem nebo SMS) a zobrazovaných v *Administration Console* (sekce *Stav* → *Výstrahy*) je dán tzv. šablonami. Šablony jsou předdefinované zprávy, ve kterých jsou určité informace (např. uživatelské jméno, IP adresa, počet spojení, informace o viru apod.) nahrazeny speciálními proměnnými. Za tyto proměnné pak *WinRoute* při odesílání zprávy dosadí konkrétní hodnoty. Správce *WinRoute* může šablony libovolně upravovat a přizpůsobit tak podobu jednotlivých zpráv dle potřeby a vkusu.

Jednotlivé šablony jsou uloženy v podadresáři `templates` instalačního adresáře *WinRoute*

(typicky `C:\Program Files\Kerio\WinRoute Firewall\templates`):

- podadresář `console` — zprávy zobrazované v horní části sekce *Stav* → *Výstrahy* (přehled),
- podadresář `console\details` — zprávy zobrazované v dolní části sekce *Stav* → *Výstrahy* (podrobnosti),
- podadresář `email` — zprávy zasílané e-mailem (každá šablona obsahuje zprávu v prostém textu a formátovanou HTML),
- podadresář `sms` — SMS zprávy zasílané na mobilní telefon.

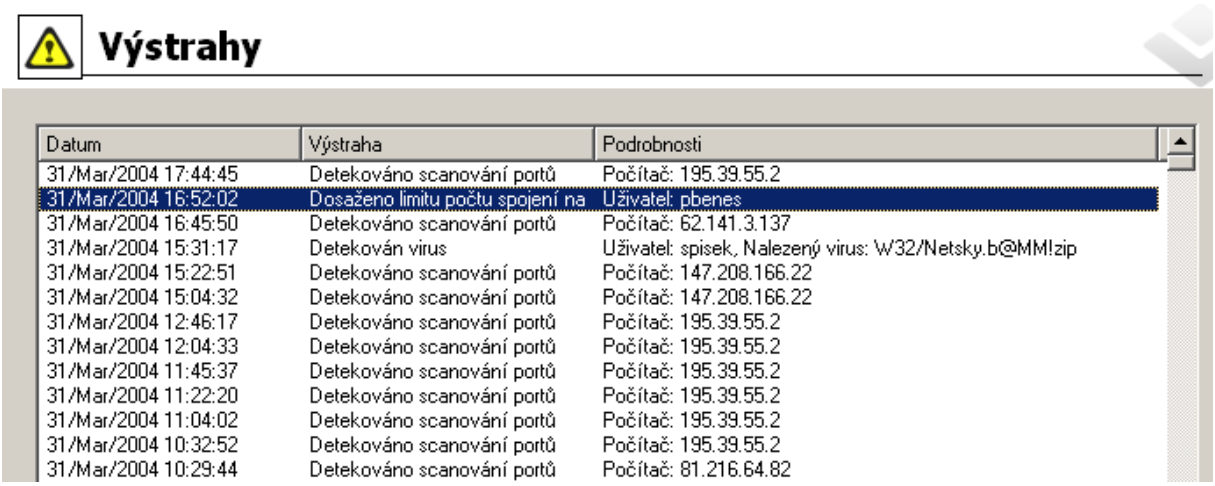
V *Administration Console* se výstrahy zobrazují v aktuálně nastaveném jazyce (viz manuál *Kerio Administration Console — Nápověda*). Nejsou-li k dispozici šablony výstrah v požadovaném jazyce, použije se angličtina. E-mailem a SMS se výstrahy zasílají vždy v angličtině.

Poznámka: V současné verzi *WinRoute* jsou šablony výstrah k dispozici pouze v anglickém a českém jazyce.

Zobrazení výstrah v Administration Console

V sekci *Stav* → *Výstrahy* lze zobrazit všechny odeslané výstrahy (definované v sekci *Konfigurace* → *Statistiky a záznamy*). Výstrahy jsou zobrazovány v jazyce *Administration Console* (není-li nalezena šablona výstrahy v odpovídajícím jazyce, pak je výstraha zobrazena v angličtině).

V horní části této sekce je uveden seznam všech odeslaných výstrah (seřazený podle dat a časů, kdy jednotlivé události nastaly).



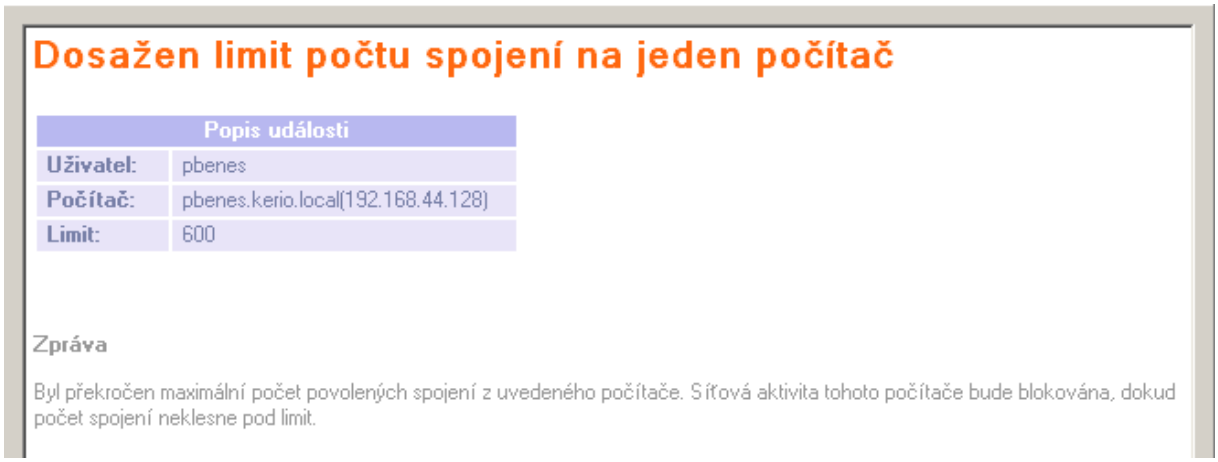
Obrázek 19.13 Přehled odeslaných výstrah

Na každém řádku je zobrazena jedna výstraha:

- *Datum* — datum a čas, kdy nastala příslušná událost,
- *Výstraha* — typ zachycené události,
- *Podrobnosti* — základní informace o události (IP adresa počítače, jméno uživatele, název viru atd.).

Po kliknutí na vybranou výstrahu se v dolní části sekce *Výstrahy* zobrazí podrobné informace o příslušné události včetně textového popisu (dle šablon v adresáři `console\details` — viz výše).

Poznámka: Podrobnosti o vybraném události lze volitelně skrýt nebo zobrazit tlačítkem v pravém dolním rohu okna (ve výchozím nastavení jsou podrobnosti zobrazeny).



Obrázek 19.14 Podrobnosti o vybrané události

Kapitola 20

Základní statistiky

Ve *WinRoute* můžeme sledovat statistické informace o uživatelích (objem přenesených dat, používané služby, kategorizace navštívených WWW stránek) a síťových rozhraních firewallu s *WinRoute* (objem přenesených dat, zatížení linek).

V programu *Administration Console* lze zobrazit informace o kvótě jednotlivých uživatelů (objem přenesených dat a využití kvóty) a statistiky síťových rozhraní (přenesená data, grafy zatížení). Podrobné statistiky uživatelů, WWW stránek a objemu přenesených dat jsou k dispozici ve WWW rozhraní firewallu (*Kerio StaR* — viz kapitola 21).

20.1 Objem přenesených dat a využití kvóty

Záložka *Statistiky uživatelů* sekce *Stav* → *Statistiky* obsahuje podrobnou statistiku objemu dat přenesených jednotlivými uživateli v každém směru za určitá časová období (dnes, tento týden, tento měsíc a celkově).

Sloupec *Kvóta* zobrazuje procentuální využití kvóty objemu přenesených dat příslušným uživatelem (viz kapitola 15.1). Pro vyšší názornost je míra využití kvóty barevně rozlišena:

- zelená barva — 0%–74%
- žlutá barva — 75%–99%
- červená barva — 100% (uživatel dosáhl limitu)

Poznámka:

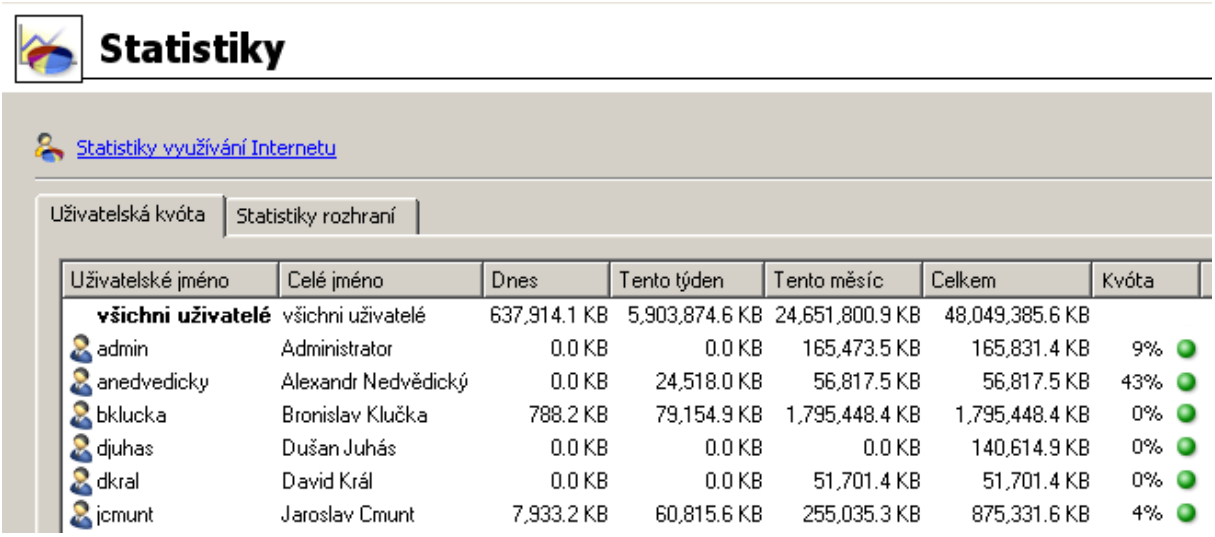
1. Uživatelská kvóta se skládá ze tří limitů: denního, týdenního a měsíčního. Ve sloupci *Kvóta* se zobrazuje vždy nejvyšší hodnota z procentuálních naplnění těchto limitů (je-li např. denní limit naplněn na 50%, týdenní na 90% a měsíční na 70%, pak se ve sloupci *Kvóta* zobrazí hodnota *90%* označená žlutou barvou).

2. Měsíční kvóta je nulována vždy na začátku tzv. účtovacího období. Toto období se může lišit od kalendářního měsíce (viz kapitola 21.2).

Řádek *všichni uživatelé* představuje souhrn za všechny uživatele v tabulce (včetně neidentifikovaných). Řádek *neidentifikovaní uživatelé* zahrnuje všechny uživatele, kteří nejsou na firewall přihlášeni. V těchto řádcích tabulky není uvedena informace o využití kvóty.

Poznámka:

1. V tabulce lze volitelně zobrazit další sloupce, obsahující objem přenesených dat za jednotlivá období v každém směru. Směr přenosu dat je vždy vztahován k příslušnému uživateli



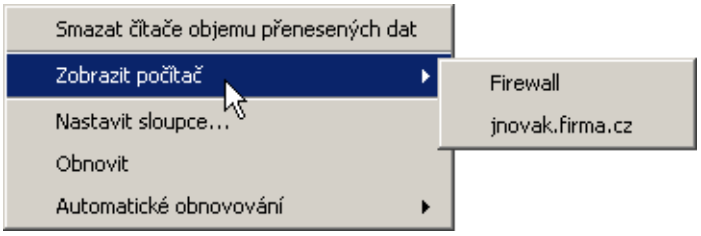
Obrázek 20.1 Statistiky uživatelů

(směr *IN* znamená data přijatá tímto uživatelem, směr *OUT* data vyslaná tímto uživatelem). Nastavení zobrazovaných sloupců je popsáno v kapitole 3.2.

2. Údaje o přeneseném objemu dat jednotlivých uživatelů jsou ukládány do souboru `stats.cfg` v adresáři *WinRoute*. Při ukončení a novém spuštění *WinRoute Firewall Engine* tedy zůstávají uchovány.

Volby pro okno Uživatelská kvóta

Po kliknutí pravým tlačítkem v tabulce (resp. na řádek s vybraným uživatelem) se zobrazí kontextové menu s těmito funkcemi:



Obrázek 20.2 Kontextové menu okna Uživatelská kvóta

Smazat čítače objemu přenesených dat

Odstranění vybraného řádku s údaji o konkrétním uživateli. Tato funkce je užitečná pro zpřehlednění statistik uživatelů (např. nechceme, aby se ve statistikách zobrazovaly zakázané uživatelské účty). Odebraný účet bude do přehledu automaticky opět přidán v okamžiku, kdy se změní data pro tento účet (např. povolíme účet, který byl zablokován, uživatel se znovu přihlásí a začne komunikovat).

Upozornění

Použitím této volby v řádku *všichni uživatelé* se vynulují čítače všech uživatelů (včetně nepřihlášených)!

Poznámka: Hodnoty objemů přenesených dat se používají také pro kontrolu uživatelské kvóty (viz kapitola 15.1). Vynulováním statistik proto dojde také k odblokování příslušného uživatele, je-li jeho komunikace blokována v důsledku překročení kvóty.

Zobrazit počítač...

Tato volba je k dispozici pouze pokud je vybraný uživatel právě přihlášen k firewallu. Volba *Zobrazit počítač* přepne zobrazení do sekce *Stav* → *Aktivní počítače* a označí počítač, ze kterého je daný uživatel přihlášen.
Je-li uživatel přihlášen z více počítačů současně, pak volba *Zobrazit počítač* otevře submenu se seznamem všech počítačů, ze kterých je daný uživatel přihlášen.

Obnovit

Okamžité obnovení informací v záložce *Statistiky uživatelů* (tato funkce je identická s funkcí tlačítka *Obnovit* v dolní části okna).

Automatické obnovování

Nastavení automatického obnovování informací v záložce *Statistiky uživatelů*. Informace mohou být automaticky obnovovány v intervalu 5 sekund — 1 minuta nebo je možné automatické obnovování vypnout (*Neobnovovat*).

Nastavit sloupce

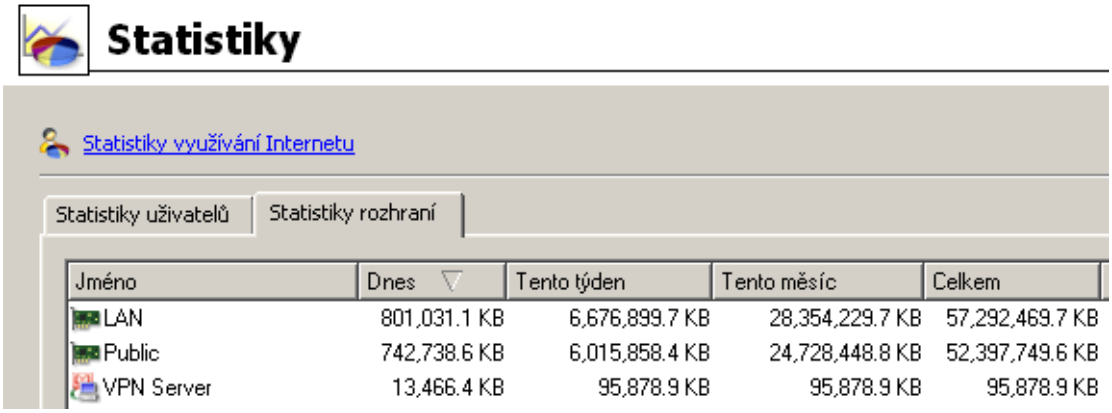
Volba sloupců, které mají být v horní části záložky *Statistiky uživatelů* zobrazeny (viz kapitola 3.2).

20.2 Statistiky rozhraní

V sekci *Stav* → *Statistiky*, záložka *Statistiky rozhraní* lze podrobně sledovat objem dat přenesených přes jednotlivá rozhraní počítače s *WinRoute* v každém směru za určitá časová období (dnes, tento týden, tento měsíc a celkově).

Rozhraní může být síťový adaptér, vytáčená linka nebo VPN tunel. Speciálním rozhraním je *VPN server* — pod ním je ve statistikách rozhraní zahrnuta komunikace všech VPN klientů.

V tabulce lze volitelně zobrazit další sloupce, obsahující objem přenesených dat za jednotlivá období v každém směru. Směr přenosu dat je vždy vztahován k příslušnému rozhraní (směr *IN* znamená data přijatá přes toto rozhraní, směr *OUT* data vyslaná přes toto rozhraní). Nastavení zobrazovaných sloupců je popsáno v kapitole 3.2.



Obrázek 20.3 Statistiky rozhraní firewallu

Příklad

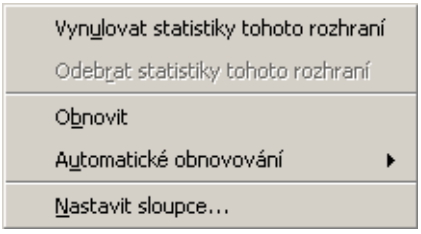
Počítač s *WinRoute* je k Internetu připojen rozhraním *Public* a lokální síť je připojená k rozhraní *LAN*. Uživatel v lokální síti stáhne z Internetu 10 MB dat. Tato data budou započtena:

- na rozhraní *Public* jako *IN* (data byla z Internetu přijata přes toto rozhraní),
- na rozhraní *LAN* jako *OUT* (data byla do lokální sítě vyslána přes toto rozhraní).

Poznámka: Statistiky rozhraní jsou ukládány do konfiguračního souboru `stats.cfg` v instalačním adresáři *WinRoute*. Při ukončení a novém spuštění *WinRoute Firewall Engine* tedy nedochází k jejich vynulování.

Volby pro okno Statistiky rozhraní

Po kliknutí pravým tlačítkem v tabulce (resp. na řádek s vybraným rozhraním) se zobrazí kontextové menu s těmito funkcemi:



Obrázek 20.4 Kontextové menu pro statistiky rozhraní

Vynulovat statistiky tohoto rozhraní
: Vynulování všech hodnot pro vybrané rozhraní. Tato funkce je aktivní, pouze je-li kurzor myši umístěn na řádku s některým rozhraním.

Obnovit
: Okamžité obnovení informací v záložce *Statistiky rozhraní* (tato funkce je identická s funkcí tlačítka *Obnovit* v dolní části okna).

Automatické obnovování

Nastavení automatického obnovování informací v záložce *Statistiky rozhraní*. Informace mohou být automaticky obnovovány v intervalu 5 sekund — 1 minuta nebo je možné automatické obnovování vypnout (*Neobnovovat*).

Nastavit sloupce

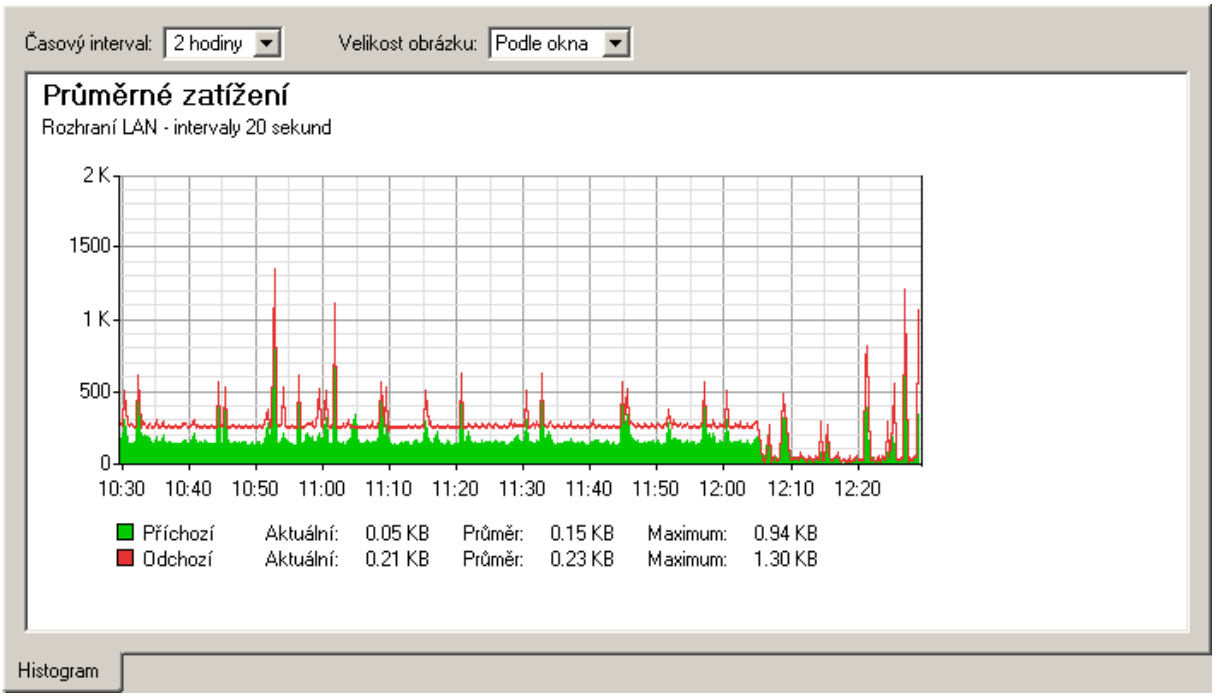
Volba sloupců, které mají být v horní části záložky *Statistiky rozhraní* zobrazeny (viz kapitola 3.2).

Odebrat statistiky tohoto rozhraní

Vyřazení vybraného rozhraní ze statistik. Odebrat lze pouze neaktivní rozhraní (tj. nepřipojený síťový adaptér, vytáčenou linku v zavěšeném stavu, nepřipojený VPN tunel nebo VPN server, ke kterému není připojen žádný klient). Pokud se odebrané rozhraní později opět aktivuje (dojde k vytočení modemu, připojení VPN tunelu atd.), bude toto rozhraní do statistik opět automaticky přidáno.

Grafický průběh zatížení rozhraní

Ve spodní části záložky *Statistiky rozhraní* se graficky zobrazuje průběh zatížení vybraného síťového rozhraní (přenosová rychlost v bytech za sekundu, *B/s*) za zvolené časové období. Graf lze skrýt a opět zobrazit tlačítkem *Skrýt podrobnosti / Zobrazit podrobnosti* (ve výchozím nastavení je graf zobrazen).



Obrázek 20.5 Graf průměrného zatížení vybraného rozhraní

V položce *Časový interval* lze vybrat časové období, které bude v grafu zobrazeno (*2 hodiny* nebo *1 den*). Zvolené časové období je vždy bráno od aktuálního času do minulosti („poslední 2 hodiny“, resp. „posledních 24 hodin“).

Vodorovná osa grafu představuje čas a svislá osa rychlost přenosu. Měřítko vodorovné osy je určeno vybraným časovým intervalem a měřítko svislé osy je nastavováno automaticky podle maximální hodnoty ve sledovaném intervalu (základní jednotkou jsou byty za sekundu — *B/s*).

Volba *Velikost obrázku* umožňuje nastavit pevnou velikost grafu nebo přizpůsobit jeho velikost oknu *Administration Console*.

Komentář nad grafem zobrazuje interval vzorkování (tj. interval, za který se hodnoty sečtou a zaznamenají do grafu).

Příklad

Je-li zvolen časový interval *1 den*, provádí se vzorkování po 5 minutách. To znamená, že se každých 5 minut do grafu zaznamená průměrná přenosová rychlost za uplynulých 5 minut.

Kapitola 21

Kerio StaR - statistiky a reportování

WinRoute poskytuje prostřednictvím WWW rozhraní podrobné statistické informace o uživatelích, objemu přenesených dat, navštívených WWW stránkách a kategoriích stránek. Tyto informace lze využít např. pro sledování pracovních a nepracovních aktivit jednotlivých uživatelů.

Statistiky sledují komunikaci mezi lokální sítí a Internetem. Objemy dat přenesených mezi počítači v lokální síti a navštívené stránky na lokálních serverech nejsou do statistik zahrnovány (ani to není technicky možné).

Výhodou webových statistik a reportů je jejich snadná dostupnost. Uživatel (typicky vedoucí pracovník) nepotřebuje program *Administration Console* a nemusí mít práva ke správě *WinRoute* (přístup ke statistikám je řízen speciálním právem). Statistiky zobrazené ve webovém prohlížeči je možné i vytisknout nebo uložit na disk jako WWW stránku.

Poznámky:

1. Správce *WinRoute* by měl informovat uživatele o tom, že jejich aktivita je na firewallu sledována.

2. Statistiky a reporty ve *WinRoute* mají informativní charakter. Nedoporučujeme je používat např. pro přesné rozúčtování nákladů na internetové připojení na jednotlivé uživatele.

3. Pro správnou funkci rozhraní *Kerio StaR* musí operační systém počítače s *WinRoute* podporovat všechny jazyky, které budou v rozhraní *Kerio StaR* používány. Pro některé jazyky (např. japonština a čínština) může být vyžadována instalace podpůrných souborů. Bližší informace naleznete v dokumentaci k příslušnému operačnímu systému.

Tato kapitola se zabývá nastavením statistik v administračním programu *WinRoute*. Samotné rozhraní *Kerio StaR* je podrobně popsáno v manuálu *Kerio WinRoute Firewall — Příručka uživatele*.

21.1 Sledování a ukládání statistických dat

Pro sledování výše popsaných statistik musí *WinRoute* získávat data různého typu. Tato data se uchovávají v databázi (podadresář `star\data` v instalačním adresáři *WinRoute* — podrobnosti viz kapitola 25.1). Celkovou dobu, pro kterou *WinRoute* statistiky uchovává, lze nastavit v *Administration Console* v sekci *Statistiky a záznamy* (viz kapitola 21.2). Výchozí nastavení je *24 měsíců* (tj. 2 roky).

WinRoute Firewall Engine z technických důvodů uchovává získaná statistická data ve své vyrovnávací paměti (cache — podadresář `star\cache`) a zápis do databáze probíhá vždy 1x za

hodinu. Cache je fyzicky reprezentována několika soubory na disku. Z toho vyplývá, že i při zastavení *WinRoute Firewall Engine*, při výpadku napájení apod. zůstanou data v cache uchována, přestože dosud nebyla zapsána do databáze.

Pro zobrazování statistik se používají data z hlavní databáze. Aktuální komunikace uživatele (např. přístup na WWW stránku) se tedy ve statistikách neprojeví ihned, ale až po skončení příslušné periody a zápisu dat do databáze.

Poznámka: Data z databáze pro statistiky nelze ručně mazat (taková akce nemá příliš velký praktický význam). Při zobrazování statistik můžeme vždy zvolit pouze takové období, které nás skutečně zajímá. Nechceme-li uchovávat stará data, můžeme zkrátit dobu uchovávání statistik (viz výše).

Podmínky pro sledování statistik

Mají-li být k dispozici všechny statistiky, musí být splněno několik základních podmínek:

- Firewall by měl vždy vyžadovat ověření uživatele. Pokud bude povolen přístup do Internetu nepřihlášeným uživatelům, statistiky dle jednotlivých uživatelů nebudou objektivní. Podrobnosti viz kapitola 10.
- Pro sledování navštěvovaných WWW stránek musí být veškerá komunikace protokolem *HTTP* obsluhována příslušným inspekčním modulem. Tato podmínka je implicitně splněna, pokud nejsou definována komunikační pravidla, která inspekční modul vyřazují (viz kapitola 7.7).
  Při použití proxy serveru ve *WinRoute* sleduje navštěvované stránky přímo proxy server (viz kapitola 8.4).
  Poznámka: Komunikace protokolem *HTTPS* je šifrována, a proto nelze sledovat navštívené stránky a kategorie stránek. Do statistik je zahrnován pouze objem přenesených dat.
- Pro sledování kategorií navštívených WWW stránek musí být také aktivní modul *Kerio Web Filter*. V konfiguraci tohoto modulu by měla být zapnuta volba *Kategorizovat každou stránku bez ohledu na pravidla pro HTTP* (jinak nebudou statistiky kategorií objektivní). Podrobnosti viz kapitola 12.3.

Sledování statistik a mapované služby

Přístup z Internetu k mapované službě na počítači v lokální síti (případně ke službě na firewallu zpřístupněné z Internetu — viz kapitola 7.3) se rovněž zahrnuje do statistik uživatelů. Je-li z daného počítače přihlášen k firewallu některý uživatel, pak je přístup k mapované službě považován za aktivitu tohoto uživatele. V opačném případě bude tento přístup zahrnut pod nepřihlášené uživatele.

Praktický význam této vlastnosti objasníme na jednoduchém příkladu. Uživatel *jnovak* je přihlášen k firewallu ze své pracovní stanice v lokální síti. Na firewallu je mapována služba *RDP* na tuto stanici, aby na ní uživatel mohl pracovat vzdáleně. Pokud se uživatel *jnovak* připojí z Internetu ke vzdálené ploše na své pracovní stanici, bude toto spojení a (data jím přenesená) zahrnuto do statistik a kvóty tohoto uživatele, protože se skutečně jedná o jeho aktivitu.

Jiným případem je veřejně přístupný mapovaný WWW server. K tomuto serveru se může připojit libovolný (anonymní) uživatel z Internetu. WWW server je však ve většině případů provozován na vyhrazeném počítači, na kterém žádný uživatel nepracuje. Proto bude veškerá komunikace s tímto serverem zahrnuta pod „nepřihlášené uživatele“.

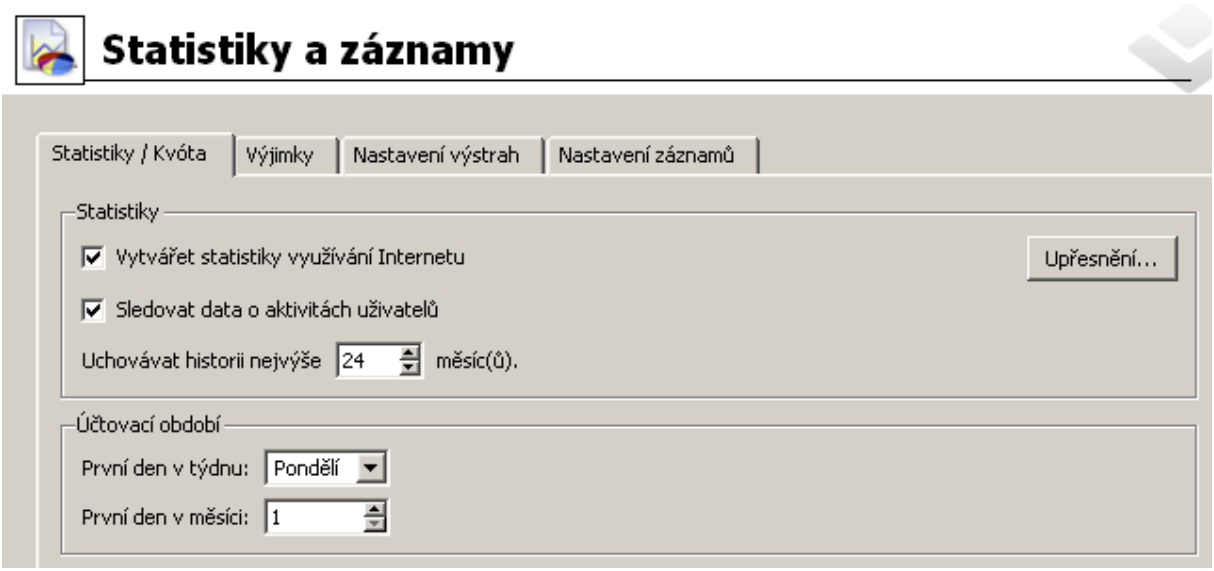
Pokud by se však z WWW serveru nějaký uživatel přihlásil k firewallu, pak by se komunikace klientů z Internetu s WWW serverem započítávala do aktivity tohoto uživatele. Pokud by navíc tento uživatel překročil svou kvótu objemu dat, pak by na tento WWW server také aplikovala příslušná omezení (viz kapitoly 15.2 a 9.2).

21.2 Nastavení statistik a kvóty

Sledování statistik může za určitých okolností (vysoký počet uživatelů, velký objem přenášených dat, nízký výkon počítače s *WinRoute* apod.) zpomalovat činnost *WinRoute* a rychlost internetového připojení. *WinRoute* proto umožňuje nastavit parametry statistik tak, aby byla shromažďována jen taková data a vytvářeny jen takové statistiky, které nás skutečně zajímají. Pokud nechceme statistiky sledovat, můžeme zakázat jejich vytváření. Ušetříme tím výkon procesoru a diskový prostor počítače s *WinRoute*.

Nastavení statistik rovněž ovlivňují sledování uživatelské kvóty objemu přenesených dat (viz kapitoly 15.1 a 20).

V sekci *Konfigurace* → *Statistiky a záznamy*, záložka *Statistiky / Kvóta*, lze nastavit sledování statistik a účtovací období pro statistiky a kvótu.



Obrázek 21.1 Nastavení statistik a účtovacího období

Sledování statistik

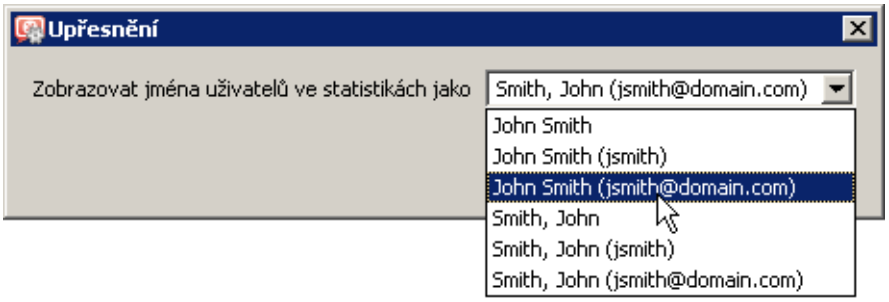
Volba *Vytvářet statistiky využívání Internetu* zapíná/vypíná sledování všech statistik (resp. sběru dat, ze kterých se statistiky vytvářejí).

Volba *Sledovat data o aktivitách uživatelů* zapíná sledování podrobných informací o aktivitě jednotlivých uživatelů. V případě, že nás informace o aktivitách uživatelů nezajímají, doporučujeme tuto volbu vypnout (sníží se zátěž firewallu a ušetří se diskový prostor serveru).

Parametrem *Uchovávat historii...* lze specifikovat období, po které budou data archivována, tzn. jaká nejstarší data budou k dispozici. Tato volba má největší vliv na potřebný diskový prostor pro statistická data. Doporučujeme nastavit pouze takové období, po které skutečně potřebujete mít statistiky uchované.

Upřesňující nastavení pro statistiky

Tlačítko *Upřesnění* otevírá dialog pro nastavení parametrů pro zobrazování statistik v rozhraní *Kerio StaR* (viz kapitola 20).



Obrázek 21.2 Upřesňující nastavení pro Kerio StaR

Volba *Zobrazovat jména uživatelů...* umožňuje zvolit způsob zobrazování jmen uživatelů v individuálních statistikách. Celé jméno uživatele může být zobrazováno ve formátu *jméno příjmení* nebo *příjmení, jméno*. Volitelně lze za celým jménem zobrazit také uživatelské jméno nebo uživatelské jméno včetně domény (je-li použito mapování domén *Active Directory*).

Účtovací období pro statistiky a kvótu

Účtovací období je časový úsek, za který se vyhodnocuje objem přenesených dat a další sumární údaje. Ve statistikách lze vytvářet týdenní a měsíční přehledy. Volbami v sekci *Účtovací období* můžeme definovat počátek týdenních a měsíčních období (např. měsíc ve statistikách může začínat 15. den kalendářního měsíce a končit 14. den následujícího kalendářního měsíce).

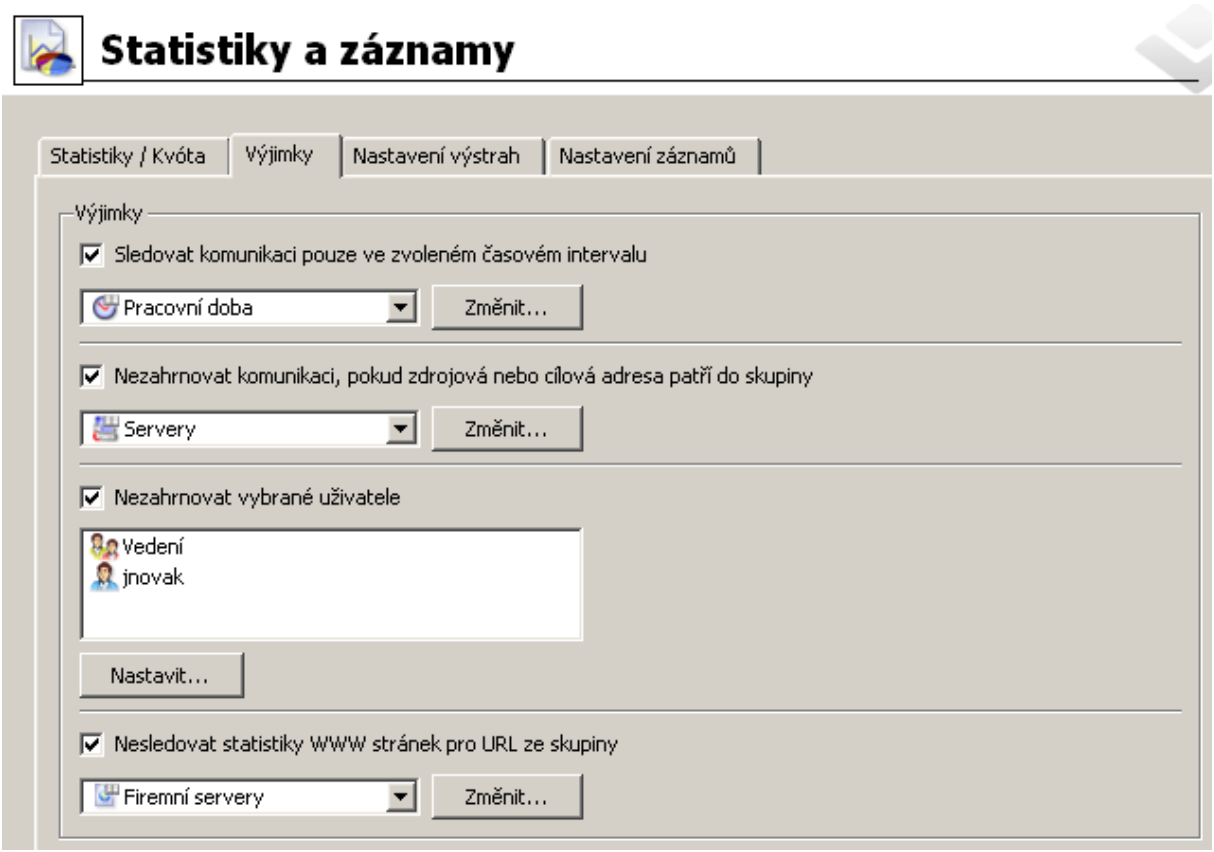
Nastavení měsíčního účtovacího období rovněž určuje, kdy bude uživatelům nulován měsíční objem přenesených dat pro kontrolu měsíční kvóty — viz kapitola 15.2.

Poznámka: Nastavení účtovacího období nemá žádný vliv na rotaci záznamů (viz kapitola 22.1).

Výjimky pro statistiky a kvótu objemu přenesených dat

V záložce *Výjimky* lze nastavit společné výjimky pro sledování statistik a pro kvótu objemu přenesených dat.

Smyslem těchto výjimek je nesledovat zbytečně informace, které z nějakého důvodu nejsou relevantní. Tím se statistiky zpřehlední a zároveň se eliminuje sběr a ukládání zbytečných dat.



Obrázek 21.3 Výjimky pro statistiky a kvótu objemu přenesených dat

Způsob použití jednotlivých výjimek:

Časový interval
: Definujeme časové období, kdy mají být statistiky a kvóta sledovány (např. pouze v pracovní době). Mimo toto období nebude žádná komunikace zahrnuta do statistik ani do kvóty.
Podrobnosti o časových intervalech viz kapitola 14.2.

IP adresy
: Definujeme IP adresy počítačů, pro které nebudou sledovány statistiky a nebude na ně aplikována kvóta.
Vybraná skupina může obsahovat IP adresy počítačů v lokální síti i v Internetu. Patří-li daná IP adresa do lokální sítě, znamená to, že do statistik a kvóty nebude zahrnuta žádná komunikace tohoto počítače. Jedná-li se o adresu serveru v Internetu, pak komunikace s tímto serverem nebude zahrnuta do statistik a kvóty žádného uživatele.

Podrobnosti o skupinách IP adres viz kapitola 14.1.

Uživatelé a skupiny

Vybereme uživatele a/nebo skupiny uživatelů, pro které nebudou sledovány statistiky a nebude na ně aplikována kvóta objemu dat. Přitom nezáleží na nastavení kvóty objemu dat v konkrétním uživatelském účtu či skupině — toto „vyřazení“ má vyšší prioritu.
Podrobnosti o uživatelích a skupinách viz kapitola 15.

WWW stránky

Definujeme skupinu URL. Přístupy na WWW stránky na těchto URL nebudou zaznamenány do statistik. Tuto výjimku lze využít např. pro vyřazení firemních WWW serverů ze statistik (přístup na WWW stránky vlastní firmy je zpravidla pracovní aktivita) nebo pro vyřazení reklam (při přístupu na určitou stránku se reklamy načítají automaticky, nejedná se o přímý požadavek uživatele). K tomuto účelu lze využít předdefinovanou skupinu URL *Ads/banners* (viz kapitola 14.4).
V položkách skupiny URL lze používat zástupné znaky. Můžeme tak definovat výjimky pro konkrétní stránky nebo pro všechny stránky na daném serveru, všechny WWW servery v dané doméně apod. Podrobnosti o skupinách URL viz kapitola 14.1.
Výjimky podle URL lze aplikovat pouze na nezabezpečené WWW stránky (protokol *HTTP*). Při přístupu na zabezpečené stránky (protokol *HTTPS*) je komunikace šifrovaná a není možné zjistit URL stránky.
Poznámka: Narozdíl od výše uvedených výjimek budou data přenesená při přístupu na tyto WWW stránky započítána do kvóty.

21.3 Přihlášení do StaR a zobrazení statistik

K prohlížení statistik je třeba se přihlásit do WWW rozhraní *WinRoute*. Uživatel (resp. skupina, do které je zařazen) musí mít právo prohlížet statistiky — viz kapitola 15.1. *StaR* lze otevřít několika způsoby v závislosti na tom, zda se chceme přihlásit přímo z počítače, na kterém je *WinRoute* nainstalován (lokální přístup) nebo z jiného počítače (vzdálený přístup).

Poznámka: Podrobnosti o WWW rozhraní *WinRoute* viz kapitola 11.2.

Přístup ke statistikám z počítače s WinRoute

Na počítači, kde je *WinRoute* nainstalován, můžeme *StaR* otevřít:

- Odkazem *Internet Usage Statistics* z kontextového menu programu *WinRoute Engine Monitor* (ikona v oznamovací oblasti nástrojové lišty — viz kapitola 2.10).
- Odkazem *Internet Usage Statistics* v menu *Start* → *Programy* → *Kerio* → *WinRoute Firewall*.

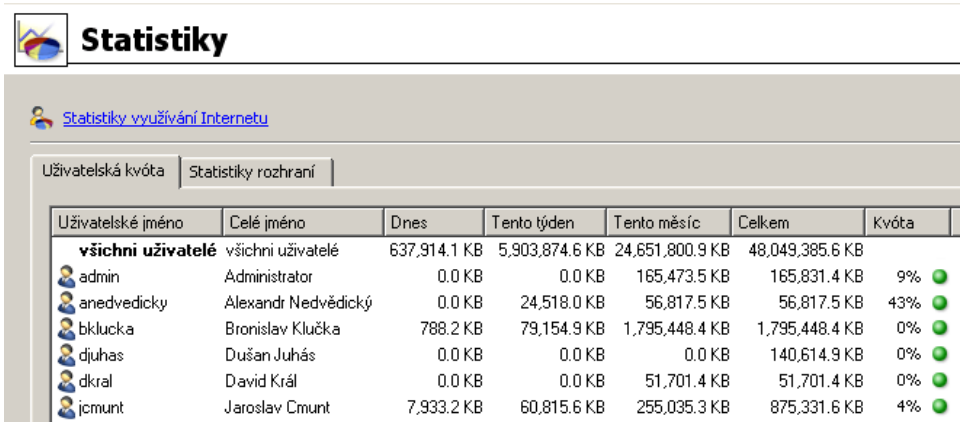
Oba tyto odkazy otevírají nezabezpečené rozhraní *StaR* na lokálním počítači (standardně `http://localhost:4080/star`) ve výchozím WWW prohlížeči.

Poznámka: V případě komunikace v rámci jednoho systému nemá použití zabezpečení smysl a WWW prohlížeč by zobrazoval zbytečná varování.

Přístup ke statistikám z jiného počítače

Z libovolného počítače, ze kterého je povolen přístup k počítači s *WinRoute* a portům WWW rozhraní je možné přistupovat ke statistikám těmito způsoby:

- Pokud jsme k *WinRoute* připojeni programem *Administration Console*, pak můžeme v sekci *Stav* → *Statistiky* použít odkaz *Statistiky využívání Internetu* v záhlaví stránky. Tento odkaz otevře zabezpečené rozhraní *StaR* ve výchozím WWW prohlížeči.
  Poznámka: URL pro tento odkaz je vytvořeno ze jména serveru a portu zabezpečeného WWW rozhraní zadaných v konfiguraci (viz kapitola 11.1). Tím je zaručena funkčnost tohoto odkazu z počítače s *WinRoute* a z lokální sítě. Má-li odkaz *Statistiky využívání Internetu* funkční i při vzdálené správě přes Internet, musí být příslušné jméno serveru uvedené ve veřejné DNS (s příslušnou veřejnou IP adresou firewallu) a komunikační pravidla musí povolovat přístup k portu zabezpečeného WWW rozhraní (standardně 4081).



Obrázek 21.4 Odkaz pro otevření webových statistik v Administration Console (sekce Stav → Statistiky)

- Na adrese `https://server:4081/star` nebo `http://server:4080/star`. Toto je URL určené výhradně pro přístup ke *StaR*. Pokud uživatel nemá právo prohlížet statistiky, zobrazí se chybová stránka.
- Na adrese `https://server:4081/`, resp. `http://server:4080/`. Toto je základní URL WWW rozhraní *WinRoute*. Pokud má uživatel právo prohlížet statistiky, zobrazí se úvodní stránka *StaR* s celkovými statistikami (viz níže). V opačném případě se zobrazí stránka *Můj účet*, která je dostupná všem uživatelům.

Upozornění

Při přístupu přes Internet (tj. z počítače mimo lokální síť) doporučujeme používat výhradně zabezpečené WWW rozhraní. Povolení přístupu z Internetu k portu nezabezpečeného WWW rozhraní by představovalo značné bezpečnostní riziko.

Aktualizace dat v rozhraní StaR

Rozhraní *StaR* je primárně určeno pro vytváření statistik a přehledů za určité období. Při sledování a vyhodnocování informací pro *StaR* musí *WinRoute* zpracovat poměrně velké množství dat. Aby nedocházelo k příliš velkému zatěžování firewallu, aktualizují se data pro *StaR* vždy cca 1x za hodinu. V pravém horním rohu každé stránky rozhraní *StaR* je vždy uvedena informace o tom, kdy proběhla poslední aktualizace těchto dat.

Z těchto důvodů není rozhraní *StaR* vhodné pro sledování aktivity uživatelů v reálném čase. Pro tyto účely doporučujeme použít sekci *Aktivní počítače* v *Administration Console* (viz kapitola 19.1).

Kapitola 22

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 (tzv. zpráva) 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). Pokud zpráva obsahuje URL, pak je zobrazeno ve formě hypertextového odkazu. Kliknutím na tento odkaz se příslušné URL otevře ve výchozím WWW prohlížeči.

Zprávy každého záznamu mohou být volitelně zapisovány do souborů na lokálním disku[7] a/nebo na *Syslog* server.

Na lokálním disku 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 *Administration Console*.

Záznamy mohou být tzv. rotovány — po uplynutí určitého období nebo při dosažení nastavené velikosti souboru je soubor záznamu archivován a záznam se začne zapisovat do nového (prázdného) souboru.

Administration Console umožňuje uložit vybraný záznam (případně jeho část) do souboru ve formátu prostý text nebo HTML. Uložený záznam lze pak dále zpracovávat různými analytickými nástroji, publikovat na WWW serveru apod.

22.1 Nastavení záznamů

K nastavení parametrů záznamů (jméno souboru, rotace, odesílání na *Syslog* server) slouží sekce *Konfigurace* → *Statistiky a záznamy*, záložka *Nastavení záznamů*. Zde je přehledně zobrazen seznam všech záznamů, které *WinRoute* používá.

Dvojitým kliknutím myší na vybraný záznam (resp. označením záznamu a stisknutím tlačítka *Změnit*) se otevírá dialog pro nastavení parametrů tohoto záznamu.

Poznámka: Nebude-li záznam ukládán do souboru na disku, pak budou v *Administration Console* zobrazovány pouze zprávy vygenerované od posledního přihlášení k *WinRoute Firewall Engine*. Po odhlášení (resp. ukončení *Administration Console*) budou tyto zprávy ztraceny.

[7] Lokálním diskem se rozumí disk počítače, na kterém je *WinRoute* nainstalován, nikoliv disk počítače, na kterém je spuštěna *Administration Console*!

Obrázek 22.1 Nastavení záznamů

Parametry pro záznam do souboru

Záložka *Záznam do souboru* umožňuje nastavení jména souboru a parametrů rotace.

Povolit záznam do souboru

Tato volba zapíná/vypíná ukládání záznamu do souboru dle položky *Jméno souboru* (k zadanému jménu bude automaticky přidána přípona `.log`).

Je-li tato volba vypnuta, jsou všechny následující položky neaktivní.

Rotovat pravidelně

Nastavení rotace v pravidelných intervalech. Tato volba způsobí rotaci záznamu (tj. archivaci souboru záznamu a zahájení zápisu do nového souboru) vždy po uplynutí zvoleného časového období.

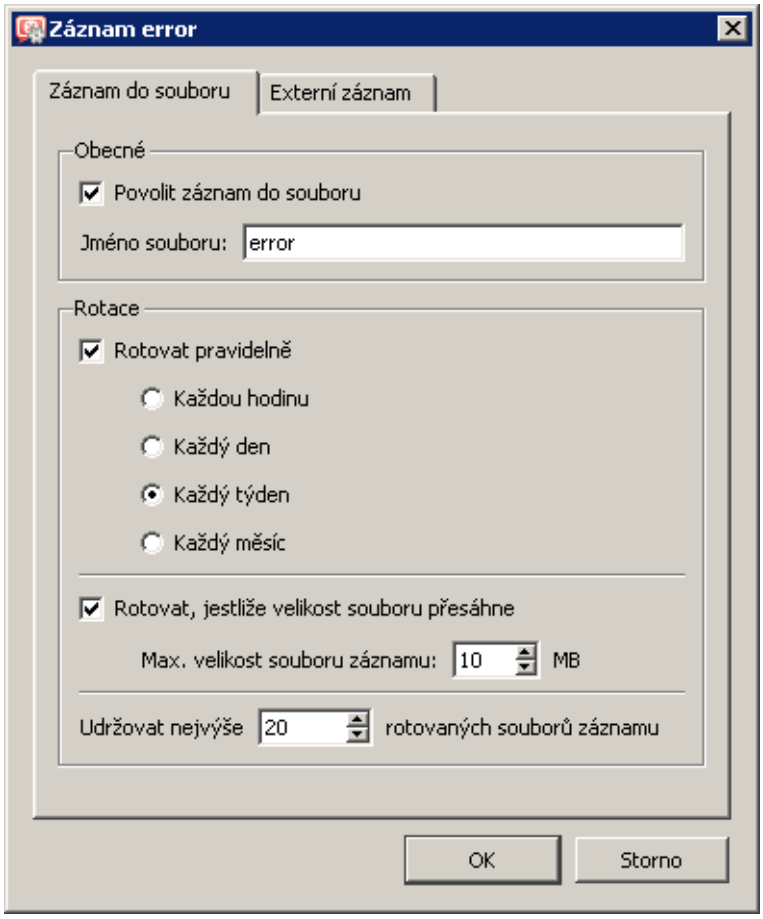
Týdenní rotace probíhá vždy o půlnoci z neděle na pondělí. Měsíční rotace probíhá vždy na přelomu posledního dne předchozího kalendářního měsíce a prvního dne následujícího měsíce.

Rotovat, jestliže velikost souboru přesáhne

Nastavení rotace při dosažení nastavené velikosti souboru záznamu. Maximální velikost souboru se zadává v megabytech (`MB`).

Uchovávat nejvýše ... souborů záznamu

Maximální počet souborů záznamu, které budou archivovány. Po dosažení tohoto počtu se při další rotaci nejstarší soubor smaže.



Obrázek 22.2 Nastavení parametrů pro záznam do souboru

Poznámka:

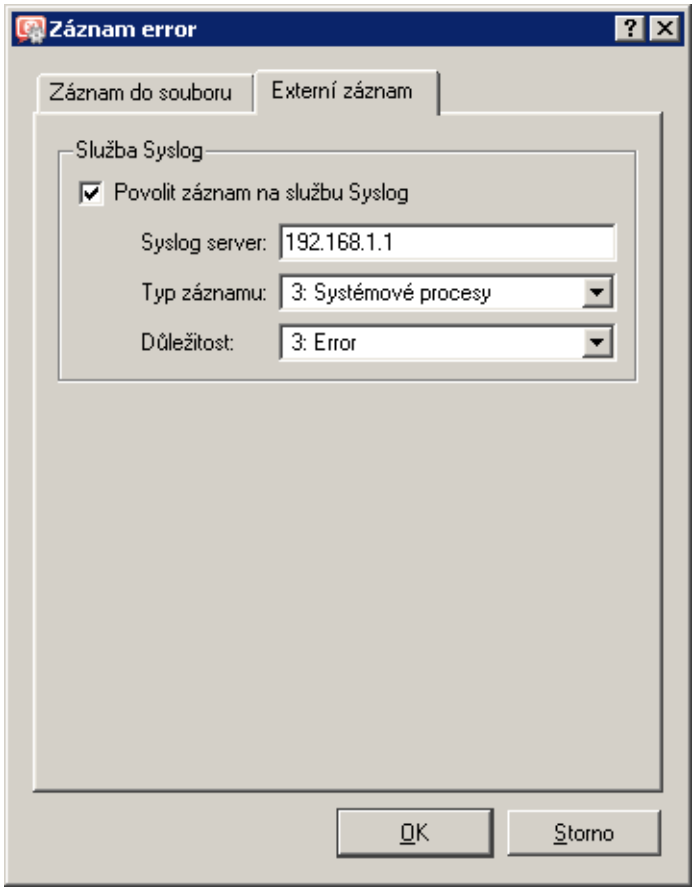
1. Jsou-li zapnuty volby *Rotovat pravidelně* a *Rotovat, jestliže velikost souboru přesáhne*, pak dojde k rotaci souboru vždy, když je splněna některá z těchto podmínek.

2. Na rotaci záznamů nemá vliv nastavení účtovacího období pro statistiky a kvótu (viz kapitola 21.2). Rotace probíhá vždy podle výše uvedených pravidel.

Nastavení záznamu na Syslog server

Záložka *Externí záznam* umožňuje nastavení parametrů pro odesílání záznamu na *Syslog* server.

Povolit záznam na službu Syslog
Zapnutí/vypnutí odesílání záznamu na *Syslog* server.
Je-li tato volba vypnuta, jsou všechny následující položky neaktivní.



Obrázek 22.3 Nastavení parametrů pro záznam na Syslog server

Syslog server
DNS jméno nebo IP adresa *Syslog* serveru.

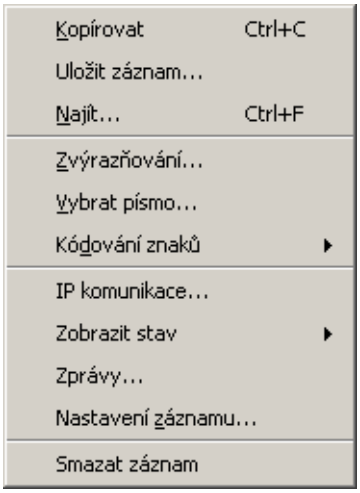
Typ záznamu
Typ zpráv, který bude použit pro daný záznam *WinRoute* (záležitost *Syslog* serveru).

Důležitost
Úroveň závažnosti zaznamenávaných zpráv (záležitost *Syslog* serveru).

22.2 Kontextové menu pro záznamy

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).

Kopírovat
Zkopírování označeného textu do schránky (clipboardu). Pro tuto funkci lze využít také klávesové zkratky operačního systému (ve *Windows Ctrl+C* nebo *Ctrl+Insert*).



Obrázek 22.4 Kontextové menu pro záznamy

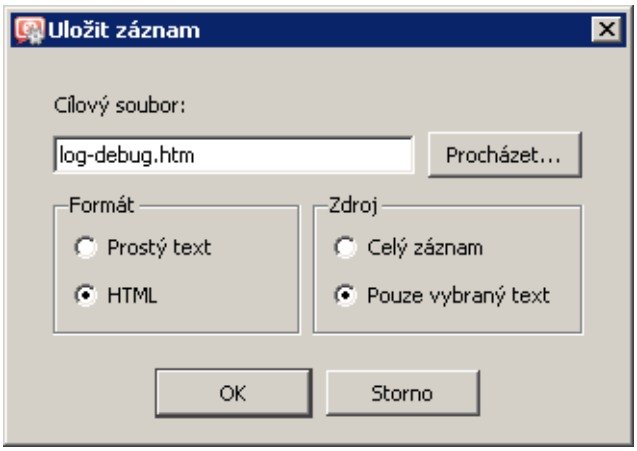
Uložit záznam

Uložení záznamu nebo označeného textu do souboru ve formátu prostý text nebo HTML.

Tip

Tato funkce umožňuje komfortnější práci se soubory záznamů než přímý přístup k souborům záznamu na disku počítače, kde je *WinRoute* nainstalován. Záznamy lze ukládat i v případě vzdálené správy *WinRoute*.

Volba *Uložit záznam* otevírá dialog pro nastavení volitelných parametrů:



Obrázek 22.5 Uložení záznamu do souboru

- *Cílový soubor* — jméno souboru, do kterého bude záznam uložen. Při otevření dialogu je přednastaveno jméno odvozené z názvu záznamu. Přípona souboru se nastavuje automaticky podle zvoleného formátu.
- *Formát* — záznam může být buď uložen jako prostý text nebo jako HTML stránka. V případě formátu HTML bude zachováno barevné zvýraznění řádků záznamu (viz sekce *Zvýrazňování zpráv v záznamech*) a všechna URL budou uložena ve formě hypertextových odkazů.
- *Zdroj* — do souboru může být uložen celý záznam nebo pouze označený text.

Upozorňujeme, že v případě vzdálené správy může uložení celého záznamu trvat až několik desítek sekund.

Najít
Vyhledání zadaného řetězce v záznamu. Záznam lze prohledávat od aktuální pozice směrem *Nahoru* (tzn. ke starším zprávám) nebo *Dolů* (tj. k novějším zprávám).
Při prvním vyhledávání (po přepnutí do okna záznamu) se záznam prochází od začátku (resp. od konce — v závislosti na zvoleném směru vyhledávání). Další vyhledávání začíná od označeného textu (text lze označit myší nebo může být označen jako výsledek předchozího vyhledávání).

Zvýrazňování
Nastavení barevného zvýraznění řádků záznamu vyhovujících určitým podmínkám (podrobnosti viz níže).

Vybrat písmo
Dialog výběru písma pro zobrazení záznamu. K dispozici jsou všechna písma instalovaná na počítači, kde je spuštěna *Administration Console*.

Kódování znaků
Výběr kódování, které bude použito pro zobrazení záznamu v programu *Administration Console*. Výchozí kódování je *UTF-8*.

Tip

Pokud se v záznamu nezobrazují korektně české znaky, zkuste zvolit jiné kódování.

Nastavení záznamu
Dialog pro nastavení jména souboru záznamu, rotace záznamu a odesílání zpráv na *Syslog*. Tyto parametry lze rovněž nastavit v sekci *Konfigurace* → *Statistiky a záznamy*, záložka *Nastavení záznamů*. Podrobnosti naleznete v kapitole 22.1.

Smazat záznam
Smazání celého záznamu. Tato volba smaže celý soubor záznamu (nikoliv pouze část zobrazenou v aktuálním okně).

Upozornění

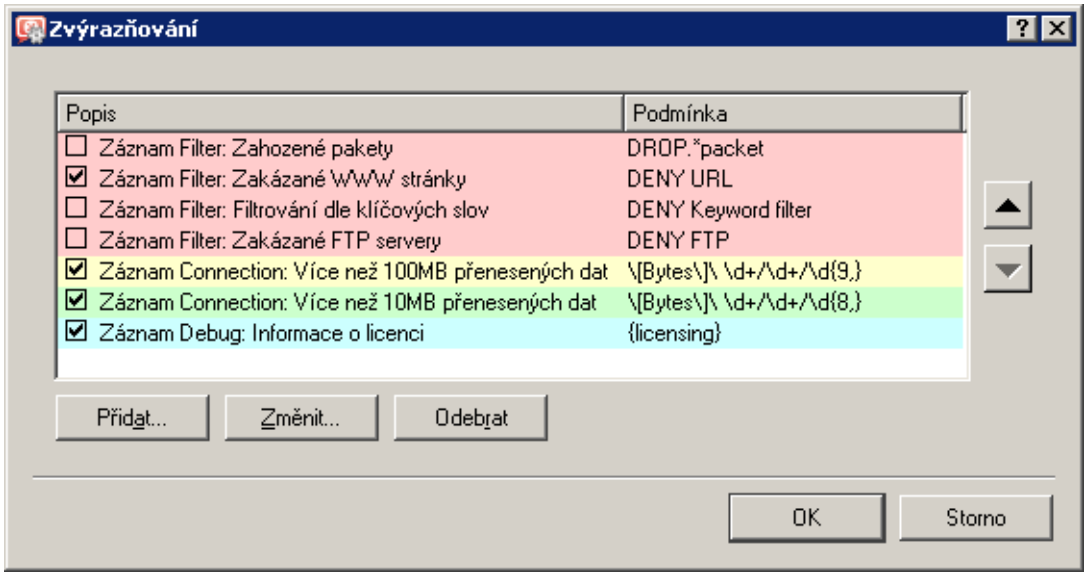
Smazaný záznam již nelze obnovit!

Poznámka: Je-li ke správě *WinRoute* přihlášen uživatel s právy pouze pro čtení (viz kapitola 15.1), pak nejsou v kontextovém menu pro záznam k dispozici volby *Nastavení záznamu* a *Smazat záznam*. Tyto akce může provádět pouze uživatel s právy pro čtení i zápis.

Zvýrazňování zpráv v záznamech

Pro snadné sledování určitých událostí je možné nastavit barevné zvýrazňování řádků záznamů vyhovujících zadaným podmínkám. Zvýrazňování definují speciální pravidla, která jsou společná pro všechny záznamy. K dispozici je 7 různých barev (+ barva pozadí, tj. nezvýrazněných řádků), počet pravidel však může být libovolný.

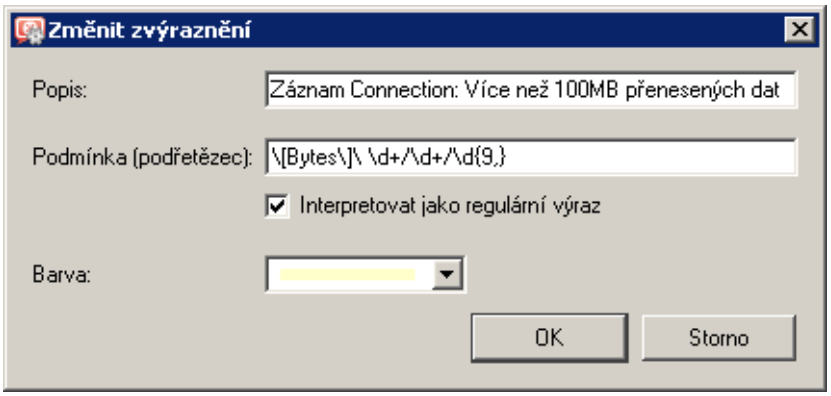
Dialog pro definici pravidel pro zvýrazňování řádků záznamu lze otevřít volbou *Zvýrazňování* z kontextového menu příslušného záznamu.



Obrázek 22.6 Nastavení zvýrazňování řádků záznamů

Zvýrazňovací pravidla tvoří uspořádaný seznam. Při zobrazování každého řádku záznamu je tento seznam vyhodnocován směrem shora dolů. Při nalezení prvního pravidla, kterému zpracovávaný řádek vyhovuje, se vyhodnocování ukončí a řádek se zvýrazní příslušnou barvou. Díky těmto vlastnostem seznamu je možné vytvářet i složitější kombinace pravidel, různé výjimky apod. Každé pravidlo lze navíc „vypnout“ nebo „zapnout“ dle potřeby (např. chceme-li dočasně zrušit některé zvýrazňování).

Tlačítko *Přidat*, resp. *Změnit* otevírá dialog pro definici zvýrazňovacího pravidla.



Obrázek 22.7 Definice pravidla pro zvýrazňování záznamů

Zvýrazňovací pravidlo sestává z podmínky a barvy, kterou budou zvýrazněny řádku záznamů vyhovující této podmínce. Podmínka může být specifikována jako podřetězec (pak budou zvýrazněny všechny řádky obsahující zadaný řetězec znaků) nebo jako tzv. regulární výraz (pak budou zvýrazněny všechny řádky obsahující jeden nebo více řetězců vyhovujících zadanému regulárnímu výrazu).

Položka *Popis* má pouze informativní charakter a slouží jen pro lepší orientaci v pravidlech.

Doporučujeme však důsledně popisovat všechna vytvořená pravidla (do popisu je vhodné uvést i jméno záznamu, na který se pravidlo vztahuje).

Poznámka: Regulární výraz je výraz, který umožňuje popsat libovolný řetězec znaků speciální symbolikou. *WinRoute* akceptuje regulární výrazy dle standardu POSIX.

Popis regulárních výrazů je nad rámec tohoto manuálu. Podrobné informace naleznete např. na adrese:

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

Speciální volby pro záznam Debug

V kontextovém menu pro záznam *Debug* jsou navíc k dispozici další volby pro nastavení sledovaných informací. Tyto volby může využít pouze uživatel s plným přístupem ke správě *WinRoute* (tj. přístupem pro čtení i zápis — viz kapitola 15.1).

Možnosti nastavení sledovaných informací v záznamu *Debug* jsou podrobně popsány v kapitole 22.6.

22.3 Záznam Alert

Záznam *Alert* obsahuje informace o všech výstrahách, které *WinRoute* generuje (např. detekce viru, vytáčení a zavěšování telefonických připojení, překročení kvóty objemu dat, detekce P2P sítě atd.).

Každá zpráva v záznamu *Alert* obsahuje časovou značku (tj. datum a čas, kdy byla zpráva zapsána) a typ výstrahy (velkými písmeny). Další položky jsou již závislé na konkrétním typu výstrahy.

Tip

V sekci *Konfigurace* → *Statistiky a záznamy* lze nastavit zasílání výstrah formou e-mailu nebo krátké textové zprávy na mobilní telefon (SMS). V sekci *Stav* → *Výstrahy* pak můžete přehledně zobrazit a procházet všechny odeslané výstrahy (podrobnosti viz kapitola 19.4).

22.4 Záznam Config

Záznam *Config* uchovává kompletní historii komunikace *Administration Console* s *WinRoute Firewall Engine* — z tohoto záznamu lze zjistit, který uživatel kdy prováděl jaké administrační úkony.

Do okna *Config* jsou zapisovány tři druhy záznamů:

1. *Informace o přihlašování uživatelů ke správě WinRoute*

Příklad

```
[18/Apr/2008 10:25:02] standa - session opened
for host 192.168.32.100

[18/Apr/2008 10:32:56] standa - session closed
for host 192.168.32.100
```

- `[18/Apr/2008 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 se uživatel připojuje
- `session closed for host 192.168.32.100` — informace o ukončení komunikace s daným počítačem (odhlášení uživatele nebo ukončení *Administration Console*)

2. *Změny v konfigurační databázi*

   Jedná se o změny provedené uživatelem v *Administration Console*. Pro komunikaci s databází se používá zjednodušená forma jazyka SQL.

Příklad

```
[18/Apr/2008 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/2008 10:27:46]` — datum a čas, kdy byl záznam zapsán
- `standa` — jméno uživatele přihlášeného ke správě *WinRoute*
- `insert StaticRoutes ...` — vložení záznamu do konfigurační databáze *WinRoute* (v tomto případě přidání statické cesty do směrovací tabulky)

3. *Ostatní konfigurační změny*

   Typickým příkladem je změna v komunikačních pravidlech. Po stisknutí tlačítka *Použít* v sekci *Konfigurace* → *Komunikační pravidla* se do záznamu *Config* vypíše kompletní seznam aktuálních komunikačních pravidel.

Příklad

```
[18/Apr/2008 12:06:03] Admin - New traffic policy set:

[18/Apr/2008 12:06:03] Admin - 1: name=(ICMP komunikace)
src=(any) dst=(any) service=("Ping")
snat=(any) dnat=(any) action=(Permit)
time_range=(always) inspector=(default)
```

- `[18/Apr/2008 12:06:03]` — datum a čas, kdy byla změna provedena
- `Admin` — jméno uživatele, který změnu provedl

- `1:` — číslo pravidla (pravidla jsou očíslována dle pořadí v tabulce shora dolů, první pravidlo má číslo 1)
- `name=(ICMP komunikace) ...` — vlastní definice pravidla (jméno, zdroj, cíl, služba atd.)

Poznámka: Implicitní pravidlo (viz kapitola 7.1) má namísto čísla označení `default`.

22.5 Záznam Connection

Záznam *Connection* obsahuje informace o spojeních odpovídajících komunikačním pravidlům se zapnutou volbou *Zaznamenat odpovídající spojení* (viz kapitola 7) nebo splňujících určité podmínky (např. záznam *UPnP* komunikace — viz kapitola 18.2).

Jak číst záznam Connection?

```
[18/Apr/2008 10:22:47] [ID] 613181 [Rule] NAT
[Service] HTTP [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/2008 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*.
- `[Rule] NAT` — jméno komunikačního pravidla, které bylo aplikováno (pravidlo, kterým byla komunikace povolena nebo zakázána).
- `[Service] HTTP` — jméno odpovídající aplikační služby (zjišťuje se podle cílového portu).
  Není-li ve *WinRoute* příslušná služba definována (viz kapitola 14.3), pak položka `[Service]` v záznamu chybí.
- `[User] standa` jméno uživatele přihlášeného k firewallu z počítače, který se účastní komunikace.
  Není-li z příslušného počítače přihlášen žádný uživatel, pak položka `[User]` v záznamu chybí.
- `[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 modulu *DNS* (viz kapitola 8.1) 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).

22.6 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.

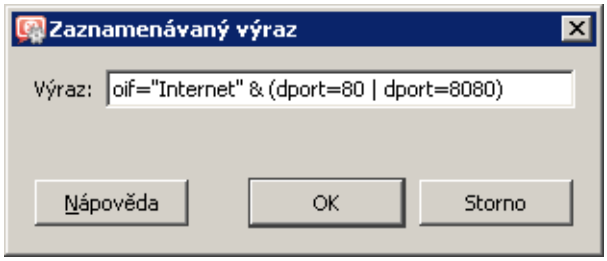
Nastavení informací zobrazovaných v záznamu Debug

V případě záznamu *Debug* obsahuje kontextové menu okna (viz kapitola 22.2) další volby umožňující podrobné nastavení záznamu nebo jednorázové zobrazení stavových informací.

Poznámka: Tyto volby jsou k dispozici pouze uživatelům s plným přístupem ke správě *WinRoute* (tj. přístupem pro čtení i zápis — viz kapitola 15.1).

IP komunikace

Sledování paketů na základě zadaného výrazu.



Obrázek 22.8 Výraz popisující komunikaci sledovanou v záznamu Debug

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.

Záznam IP komunikace lze zrušit smazáním obsahu pole *Výraz*.

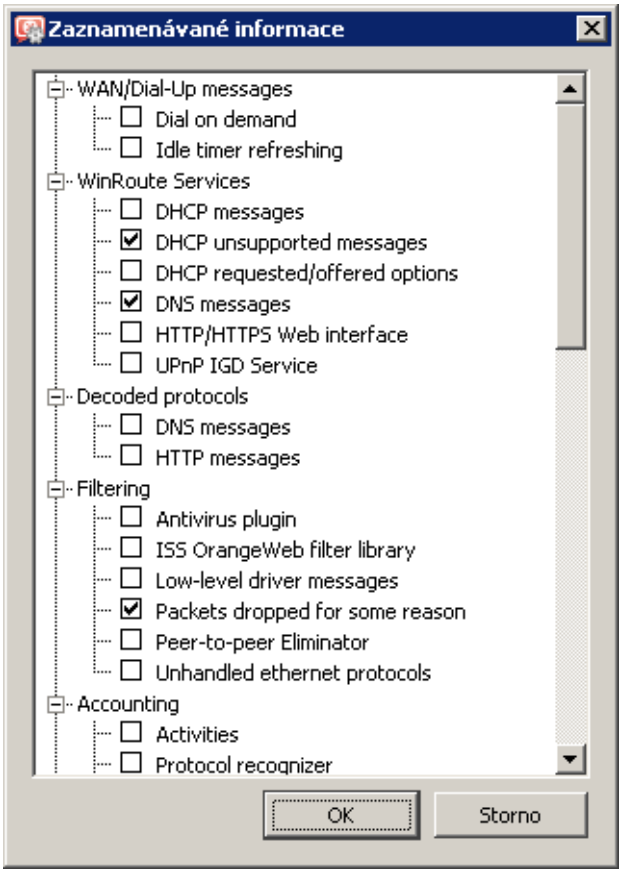
Zobrazit stav

Jednorázový výpis stavových informací některých komponent *WinRoute*. Tyto informace mají význam pouze ve speciálních případech při řešení problémů ve spolupráci s technickou podporou *Kerio Technologies*.

Zprávy

Možnost podrobného sledování funkce jednotlivých modulů *WinRoute*. Tyto informace mohou být užitečné při řešení problémů s komponentami *WinRoute* a/nebo s určitými síťovými službami.

- *WAN / Dial-up messages* — informace o vytáčených linkách (vytáčení na žádost, čítač doby automatického zavěšení),
- *Filtering* — záznamy o filtrování komunikace procházející přes *WinRoute* (antivirová kontrola, kategorizace WWW stránek, detekce a eliminace *P2P* sítí, zahozené pakety...),



Obrázek 22.9 Výběr informací sledovaných v záznamu Debug

- *Accounting* — ověřování uživatelů a sledování jejich aktivity (rozpoznávání protokolů, statistiky a reportování...),
- *WinRoute services* — protokoly zpracovávané službami *WinRoute* (*DHCP server*, modul *DNS*, WWW rozhraní a podpora protokolu *UPnP*),
- *Decoded protocols* — zobrazení obsahu zpráv vybraných protokolů (*HTTP* a *DNS*),
- *Miscellaneous* — různé další informace (např. zpracování paketů modulem *Bandwidth Limiter*, internetové připojení, HTTP cache, využití licence, kontrola aktualizací, spolupráce s dynamickým DNS...),
- *Protocol inspection* — zprávy od jednotlivých inspekčních modulů *WinRoute* (dle obsluhovaného protokolu),
- *Kerio VPN* — podrobné informace o komunikaci v rámci *Kerio VPN* (VPN tunely, VPN klienti, šifrování, výměna směrovacích informací, WWW server pro *Clientless SSL-VPN*...).

22.7 Záznam Dial

Záznam o vytáčení, zavěšování a době připojení vytáčených linek.

V záznamu *Dial* se objevují zprávy několika různých typů:

1. Ruční vytočení linky (z *Administration Console* — viz kapitola 5 nebo přímo z operačního

systému)

```
[15/Mar/2008 15:09:27] Line "Pripojeni" dialing,
console 127.0.0.1 - Admin
```

```
[15/Mar/2008 15:09:39] Line "Pripojeni" successfully connected
```

První záznam je zapsán v okamžiku zahájení vytáčení. Záznam vždy obsahuje jméno vytáčené linky ve *WinRoute* (viz kapitola 5). Pokud byla linka vytočena z *Administration Console*, obsahuje navíc tyto informace

- odkud byla linka vytočena (`console` — *Administration Console*),
- IP adresu klienta (tj. *Administration Console*),
- přihlašovací jméno uživatele, který zadal požadavek na vytočení linky.

Druhý záznam je zapsán v okamžiku úspěšného připojení (tj. po vytočení linky, ověření na vzdáleném serveru atd.).

2. Zavěšení linky (ručně nebo z důvodu nečinnosti)

   ```
   [15/Mar/2008 15:29:18] Line "Pripojeni" hang-up,
   console 127.0.0.1 - Admin
   ```

   ```
   [15/Mar/2008 15:29:20] Line "Pripojeni" disconnected,
   connection time 00:15:53, 1142391 bytes received,
   250404 bytes transmitted
   ```

   První záznam je zapsán v okamžiku přijetí požadavku na zavěšení linky. Záznam obsahuje jméno rozhraní, typ klienta, IP adresu a jméno uživatele (stejně jako v případě ručního vytáčení).

   Druhý záznam je zapsán v okamžiku úspěšného zavěšení linky. Záznam obsahuje jméno rozhraní, dobu připojení (`connection time`), objem přijatých a vyslaných dat v bytech (`bytes received` a `bytes transmitted`).

3. Zavěšení linky z důvodu chyby (přerušení spojení)

   ```
   [15/Mar/2008 15:42:51] Line "Pripojeni" dropped,
   connection time 00:17:07, 1519 bytes received,
   2504 bytes transmitted
   ```

   Význam položek záznamu je stejný jako v předchozím případě (druhý záznam — hlášení `disconnected`).

4. Vytáčení linky na žádost (na základě DNS dotazu)

   ```
   [15/Mar/2008 15:51:27] DNS query for "www.microcom.com"
   (packet UDP 192.168.1.2:4567 -> 195.146.100.100:53)
   initiated dialing of line "Pripojeni"
   ```

   ```
   [15/Mar/2008 15:51:38] Line "Pripojeni" successfully connected
   ```

   První záznam je zapsán v okamžiku vzniku DNS požadavku (modul *DNS* zjistil, že požadovaný DNS záznam se nenachází v jeho cache). Záznam obsahuje:

- DNS jméno, pro které je zjišťována IP adresa,
- popis paketu s DNS dotazem (protokol, zdrojová IP adresa, zdrojový port, cílová IP adresa, cílový port),
- jméno linky, která bude vytočena.

Druhý záznam je zapsán v okamžiku úspěšného připojení (tj. po vytočení linky, ověření na vzdáleném serveru atd.).

5. Vytáčení linky na žádost (na základě paketu z lokální sítě)

```
[15/Mar/2008 15:53:42] Packet
TCP 192.168.1.3:8580 -> 212.20.100.40:80
initiated dialing of line "Pripojeni"

[15/Mar/2008 15:53:53] Line "Pripojeni" successfully connected
```

První záznam je zapsán v okamžiku, kdy *WinRoute* zjistí, že ve směrovací tabulce neexistuje cesta, kam má být přijatý paket směrován. Záznam obsahuje:

- popis paketu (protokol, zdrojová IP adresa, zdrojový port, cílová IP adresa, cílový port),
- jméno linky, která bude vytočena.

Druhý záznam je zapsán v okamžiku úspěšného připojení (tj. po vytočení linky, ověření na vzdáleném serveru atd.).

6. Linku nelze vytočit z důvodu chyby (např. chyba modemu, odpojená telefonní linka apod.)

```
[15/Mar/2008 15:59:08] DNS query for "www.microsoft.com"
(packet UDP 192.168.1.2:4579 -> 195.146.100.100:53)
initiated dialing of line "Pripojeni"

[15/Mar/2008 15:59:12] Line "Pripojeni" disconnected
```

První záznam představuje DNS dotaz z lokální sítě, na základě kterého má být linka vytočena (viz výše).

Druhý záznam (bezprostředně následující po prvním) informuje o tom, že linka je zavěšena. Narozdíl od „normálního“ zavěšení linky zde není uvedena doba připojení a objem přenesených dat, protože linka ve skutečnosti vůbec připojena nebyla.

22.8 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.

Každý záznam v okně *Error* obsahuje kód a subkód chyby — dvě čísla v závorce za časovou značkou `(x y)`. Podle kódu chyby (`x`) rozlišujeme následující kategorie chybových hlášení:

- `1-999` — problém se systémovými zdroji (nedostatek paměti, chyba alokace paměti atd.)
- `1000-1999` — interní chyby (nelze přečíst směrovací tabulku, IP adresy rozhraní apod.)
- `2000-2999` — problémy s licencí (licence vypršela, překročen maximální počet uživatelů, nelze najít soubor s licencí atd.)
- `3000-3999` — chyby konfigurace (nelze načíst konfigurační soubor, detekována smyčka v nastavení modulu *DNS* nebo *Proxy serveru* apod.)
- `4000-4999` — síťové (socketové) chyby
- `5000-5999` — chyby při spouštění a zastavování *WinRoute Firewall Engine* (problémy s nízkoúrovňovým ovladačem, inicializací používaných systémových knihoven a služeb, konfigurační databází atd.)
- `6000-6999` — chyby souborového systému (nelze otevřít / uložit / smazat soubor)
- `7000-7999` — chyby SSL (problémy s klíči, certifikáty atd.)
- `8000-8099` — chyby HTTP cache (chyby při čtení / ukládání souborů, nedostatek volného místa na disku apod.)
- `8100-8199` — chyby modulu *Kerio Web Filter*
- `8200-8299` — chyby ověřovacího subsystému
- `8300-8399` — chyby antivirového modulu (test antiviru proběhl neúspěšně, problém s ukládáním dočasných souborů atd.)
- `8400-8499` — chyby telefonického připojení (nelze načíst definovaná připojení, chyba konfigurace linky atd.)
- `8500-8599` — chyby LDAP (nelze najít server, neúspěšné přihlášení...)

Poznámka: Je-li v záznamu *Error* opakovaně hlášena chyba, kterou nedokážete svépomocí odstranit (resp. ani zjistit její příčinu), kontaktujte technickou podporu firmy Kerio Technologies. Podrobné informace naleznete v kapitole 26 nebo na WWW stránkách `http://www.kerio.cz/`.

22.9 Záznam Filter

Záznam o WWW stránkách a objektech blokovaných, resp. povolených HTTP a FTP filtrem (viz kapitoly 12.2 a 12.5) a o paketech vyhovujících komunikačním pravidlům se zapnutou volbou *Zaznamenat odpovídající pakety* (viz kapitola 7) nebo jiným podmínkám (např. záznam *UPnP* komunikace — viz kapitola 18.2).

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 HTTP pravidlo

```
[18/Apr/2008 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/2008 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

Příklad záznamu paketu

```
[16/Apr/2008 10:51:00] PERMIT 'Lokální komunikace' 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/2008 10:51:00]` — datum a čas, kdy byl záznam zapsán
- `PERMIT` — akce, která byla provedena (`PERMIT` = povoleno, `DENY` = zakázáno, `DROP` = zahozeno)
- `Lokální komunikace` — název komunikačního pravidla, kterému paket vyhověl
- `packet to` — směr paketu (`to` = vyslaný na dané rozhraní, `from` = přijatý z daného rozhraní)
- `LAN` — jméno rozhraní, na kterém byla komunikace zachycena (podrobnosti viz kapitola 5)
- `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

22.10 Záznam Http

Kompletní záznam HTTP požadavků, které byly zpracovány inspekčním modulem protokolu HTTP (viz kapitola 14.3) nebo vestavěným proxy serverem (viz kapitola 8.4). Tento záznam má standardní formát logu WWW serveru *Apache* (viz http://www.apache.org/) nebo formát logu proxy serveru *Squid* (viz http://www.squid-cache.org/). Záznam *Http* lze zapnout

nebo vypnout a nastavit jeho typ v sekci *Konfigurace* → *Filtrování obsahu* → *Pravidla pro HTTP* (podrobnosti viz kapitola 12.2)

Poznámka:

1. Do tohoto záznamu se ukládají pouze přístupy na povolené stránky. Požadavky blokované HTTP pravidly lze sledovat v záznamu *Filter* (viz kapitola 22.9), je-li v příslušném pravidle zapnuta volba *Zaznamenat* (viz kapitola 12.2).

2. Záznam *Http* je vhodný ke zpracování externími analytickými nástroji. Pro správce *WinRoute* bude pravděpodobně přehlednější záznam *Web* (viz dále).

Příklad záznamu Http typu Apache

```
192.168.64.64 - rgabriel
[18/Apr/2008:15:07:17 +0200]
"GET http://www.kerio.cz/ HTTP/1.1" 304 0 +4
```

- `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/2008:15:07:17 +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
- `+4` —počet HTTP požadavků přenesených v rámci daného spojení

Příklad záznamu Http typu Squid

```
1058444114.733 0 192.168.64.64 TCP_MISS/304 0
GET http://www.squid-cache.org/ - DIRECT/206.168.0.9
```

- `1058444114.733` — časová značka (sekundy.milisekundy od 1.1.1970)
- `0` — doba stahování objektu (ve *WinRoute* se neměří — tato hodnota je vždy nulová)
- `192.168.64.64` — IP adresa klienta (tj. počítače, ze kterého klient k WWW stránkám přistupuje)
- `TCP_MISS` — je použit komunikační protokol TCP a objekt nebyl nalezen v cache („missed“). Ve *WinRoute* tato položka nenabývá jiné hodnoty.
- `304` — návratový kód protokolu HTTP
- `0` — objem přenášených dat v bytech (velikost objektu)
- `GET http://www.squid-cache.org/` — HTTP požadavek (metoda a URL objektu)
- `DIRECT` — způsob přístupu klienta k WWW serveru (ve *WinRoute* vždy `DIRECT` = přímý přístup)
- `206.168.0.9` — IP adresa WWW serveru

22.11 Záznam Security

Informace, které souvisejí s bezpečností *WinRoute* a lokální sítě. Záznam *Security* může obsahovat záznamy následujících kategorií:

1. *Záznamy funkce Anti-spoofing*

   Záznamy o paketech, které byly zachyceny funkcí *Anti-spoofing* (tzn. pakety s neplatnou zdrojovou IP adresou — podrobnosti viz kapitola 17.2).

   Příklad

   ```
   [17/Jul/2008 11:46:38] Anti-Spoofing:
   Packet from LAN, proto:TCP, len:48,
   ip/port:61.173.81.166:1864 -> 195.39.55.10:445,
   flags: SYN, seq:3819654104 ack:0, win:16384, tcplen:0
   ```

   - `packet from` — směr paketu (`to` = přijatý přes dané rozhraní, `from` = vyslaný přes dané rozhraní)
   - `LAN` — jméno rozhraní, na kterém byla komunikace zachycena (podrobnosti viz kapitola 5)
   - `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

2. *Zprávy inspekčního modulu protokolu FTP*

   Příklad 1

   ```
   [17/Jul/2008 11:55:14] FTP: Bounce attack attempt:
   client: 1.2.3.4, server: 5.6.7.8,
   command: PORT 10,11,12,13,14,15
   ```

   (detekován pokus o útok — klient poslal v příkazu `PORT` cizí IP adresu)

   Příklad 2

   ```
   [17/Jul/2008 11:56:27] FTP: Malicious server reply:
   client: 1.2.3.4, server: 5.6.7.8,
   response: 227 Entering Passive Mode (10,11,12,13,14,15)
   ```

   (podezřelá odpověď FTP serveru — obsahuje cizí IP adresu)

3. *Zprávy o neúspěšném ověření uživatelů*

   Formát zprávy:

   `Authentication: <služba>: Client: <IP adresa>: <důvod>`

   - `<služba>` — služba *WinRoute*, ke které se klient přihlašuje (`Admin` = správa *WinRoute* pomocí *Administration Console*, `WebAdmin` = WWW administrační rozhraní, `WebAdmin SSL` = zabezpečená verze WWW administračního rozhraní, `Proxy` = ověření uživatele na proxy serveru)
   - `<IP adresa>` — IP adresa počítače, odkud se klient pokusil přihlásit k dané službě
   - `<důvod>` — příčina neúspěšného přihlášení (neexistující uživatel / nesprávné heslo)

   Poznámka: Podrobné informace o ověřování uživatelů naleznete v kapitolách 15.1 a 10.1.

4. *Informace o startu a ukončení* WinRoute Firewall Engine.

   a) Start Engine:

   `[17/Dec/2008 12:11:33] Engine: Startup.`

   b) Ukončení Engine:

   `[17/Dec/2008 12:22:43] Engine: Shutdown.`

22.12 Záznam Sslvpn

Do tohoto záznamu jsou zapisovány operace se soubory provedené uživateli v rozhraní *Clientless SSL-VPN*. Každý řádek záznamu obsahuje typ operace, jméno uživatele, který ji provedl, a soubor, kterého se operace týkala.

Příklad

```
[17/Mar/2008 08:01:51] Copy File: User: jnovak@firma.cz
File: '\\server\data\www\index.html'
```

Rozhraní *Clientless SSL-VPN* a příslušný záznam je k dispozici pouze ve *WinRoute* pro systém *Windows*.

22.13 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.

Každé varovné hlášení má svůj číselný kód (`code xxx:`). Podle těchto kódů zpráva patří do jedné z následujících kategorií:

- `1000-1999` — systémová varování (např. detekce známé konfliktní aplikace)
- `2000-2999` — problémy s konfigurací *WinRoute* (např. pravidla pro HTTP vyžadují ověřování uživatelů, ale WWW administrační rozhraní není povoleno)
- `3000-3999` — varovná hlášení jednotlivých modulů *WinRoute* (např. DHCP server, antivirová kontrola, ověřování uživatelů atd.)
- `4000-4999` — varování týkající se licence (vypršení předplatného nebo blížící se vypršení licence *WinRoute*, modulu *Kerio Web Filter* nebo antiviru *McAfee*).
  Poznámka: Vypršení licence je považováno za chybu — tato informace se zapisuje do záznamu *Error*.

Příklad záznamů v okně Warning

```
[15/Apr/2008 15:00:51] (3004) Authentication subsystem warning:
Kerberos 5 auth: user standa@firma.cz not authenticated

[15/Apr/2008 15:00:51] (3004) Authentication subsystem warning:
Invalid password for user admin

[16/Apr/2008 10:53:20] (3004) Authentication subsystem warning:
User jnovak doesn't exist
```

- První záznam: informace o neúspěšném ověření uživatele `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`

Poznámka: V případě problémů s ověřováním uživatelů se také zapisují odpovídající informace do záznamu *Security*.

22.14 Záznam Web

Tento záznam zobrazuje HTTP požadavky zpracované inspekčním modulem protokolu HTTP (viz kapitola 14.3) nebo vestavěným proxy serverem (viz kapitola 8.4). 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/2008 10:29:51] 192.168.44.128 standa
"Kerio Technologies" http://www.kerio.cz/
```

- `[24/Apr/2008 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"` — 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 23

Kerio VPN

WinRoute umožňuje bezpečné propojení vzdálených privátních sítí šifrovaným tunelem a zabezpečený přístup klientů do lokální sítě přes Internet. Tento způsob propojení sítí (resp. přístupu vzdálených klientů do lokální sítě) se nazývá virtuální privátní síť (*VPN — Virtual Private Network*). *WinRoute* obsahuje proprietární implementaci VPN (dále jen „*Kerio VPN*“).

Implementace VPN ve *WinRoute* je navržena tak, aby ji bylo možné provozovat společně s firewallem a překladem adres (i vícenásobným) na kterékoliv straně. Vytvoření zabezpečeného tunelu mezi sítěmi a nastavení serveru pro připojování vzdálených klientů je velmi snadné.

Kerio VPN umožňuje vytvořit libovolný počet zabezpečených šifrovaných spojení typu *server-to-server* (tj. tunelů do vzdálených privátních sítí). Tunel se vytváří mezi dvěma *WinRoute*, typicky na internetových branách příslušných sítí. Jednotlivé servery (konce tunelů) se navzájem ověřují pomocí SSL certifikátů — tím je zajištěno, že tunel bude vytvořen pouze mezi důvěryhodnými servery.

K VPN serveru ve *WinRoute* se mohou připojovat také jednotlivé počítače (zabezpečené připojení typu *client-to-server*). Identita klienta je ověřována jménem a heslem (přenáší se zabezpečeným spojením), čímž je vyloučeno připojení neoprávněného klienta do lokální sítě.

Pro připojení vzdálených klientů je společně s *WinRoute* dodávána aplikace *Kerio VPN Client* (podrobné informace viz samostatný manuál *Kerio VPN Client — Příručka uživatele*).

Poznámka: Koncepce *Kerio VPN* předpokládá, že *WinRoute* je nasazen na počítači, který je výchozí bránou do Internetu. V opačném případě lze *Kerio VPN* použít, ale konfigurace je komplikovanější.

Výhody použití Kerio VPN

Ve srovnání s konkurenčními produkty pro bezpečné propojování sítí přes Internet nabízí *Kerio VPN* řadu výhod a doplňkových funkcí.

- Velmi snadná konfigurace (při vytváření tunelů a konfiguraci serverů pro připojení klientů je třeba zadat jen několik základních parametrů).
- Pro vytvoření tunelu není třeba instalovat žádný další software (vzdálení klienti potřebují aplikaci *Kerio VPN Client* — instalační archiv této aplikace má velikost cca 8 MB).
- Nedochází k problémům při vytváření zabezpečených šifrovaných kanálů přes firewall. Koncepce *Kerio VPN* předpokládá, že na cestě mezi propojovanými sítěmi (resp. mezi vzdáleným klientem a lokální sítí) může být použit firewall nebo několik firewallů (případně firewallů s překladem adres — *NAT*).

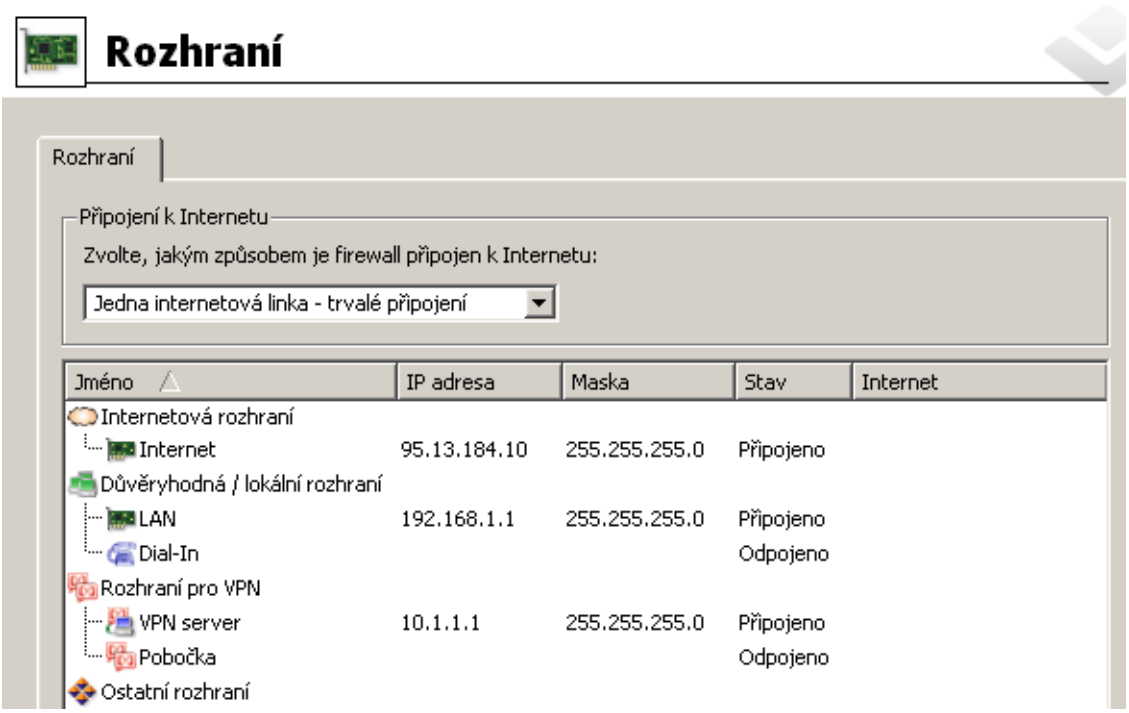
- Pro VPN klienty není třeba vytvářet speciální uživatelské účty. Pro ověřování klientů se používají uživatelské účty ve *WinRoute* (resp. přímo doménové účty při použití *Active Directory* — viz kapitola 10.1).
- Ve *WinRoute* lze sledovat statistické informace o VPN tunelech a VPN klientech, podobně jako v případě fyzických rozhraní (podrobnosti viz kapitola 20.2).

23.1 Konfigurace VPN serveru

VPN server slouží pro připojování vzdálených konců VPN tunelů a vzdálených klientů pomocí aplikace *Kerio VPN Client*.

Poznámka: Připojení k VPN serveru z Internetu musí být povoleno komunikačními pravidly. Podrobné informace naleznete v kapitolách 23.2 a 23.3.

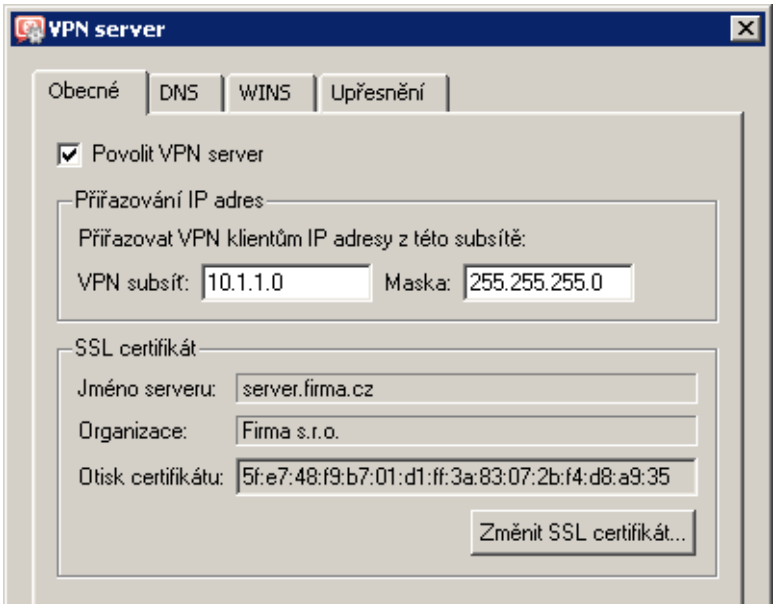
VPN server se zobrazuje jako speciální rozhraní v sekci *Konfigurace* → *Rozhraní*, záložka *Rozhraní*.



Obrázek 23.1 Zobrazení VPN serveru v tabulce rozhraní

Dvojitým kliknutím na rozhraní *VPN server* (resp. stisknutím tlačítka *Změnit*) se otevře dialog pro nastavení parametrů VPN serveru.

VPN subsít' a SSL certifikát



Obrázek 23.2 Nastavení VPN serveru — základní parametry

Povolit VPN server

Tato volba spouští / zastavuje VPN server. VPN server používá protokoly TCP a UDP, standardní port je 4090 (tento port lze změnit v upřesňujících nastaveních, výchozí hodnotu však zpravidla není třeba měnit). Nebude-li VPN server používán, doporučujeme jej vypnout.

Ke spuštění, resp. zastavení VPN serveru dojde až po stisknutí tlačítka *Použít* v záložce *Rozhraní*.

Přiřazování IP adres

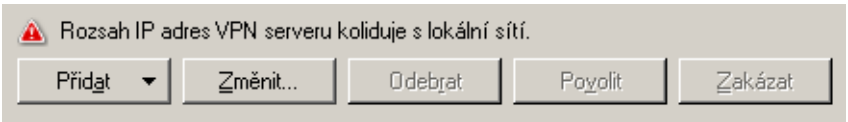
Nastavení subsítě (tj. adresy sítě s příslušnou maskou), ze které budou přidělovány IP adresy VPN klientům a vzdáleným koncům VPN tunelů připojujícím se k tomuto serveru (všichni klienti budou připojeni do této subsítě).

Ve výchozím nastavení (tzn. při prvním spuštění po instalaci) *WinRoute* vybere vhodnou volnou subsíť pro VPN. Za normálních okolností není třeba automaticky nastavenou subsíť měnit. Po provedení první změny v nastavení VPN serveru je již vždy používána naposledy zadaná subsíť (automatická detekce se již znovu neprovádí).

Upozornění

Subsíť pro VPN klienty nesmí kolidovat s žádnou lokální subsítí!

WinRoute dokáže detekovat kolizi VPN subsítě s lokálními subsítěmi. Ke kolizi může dojít při změně konfigurace lokální sítě (změna IP adres, přidání nové subsítě apod.), případně při nastavení nevhodně zvolené subsítě VPN. Překrývá-li se zadaná VPN subsíť s lokální sítí, pak se po uložení nastavení (stisknutím tlačítka *Použít* v dolní části záložky *Rozhraní*) zobrazí varovné hlášení. V takovém případě je třeba nastavit jinou VPN subsíť.



Obrázek 23.3 VPN server — detekce kolize IP adres

Po každé změně konfigurace lokální sítě nebo VPN doporučujeme pečlivě zkontrolovat, zda není hlášena kolize IP adres!

Poznámky:

1. Ke kolizi s lokální sítí může za určitých okolností dojít i při automatickém nastavení VPN subsítě (pokud bude později změněna konfigurace lokální sítě).
2. V případě VPN tunelu se při navazování spojení také kontroluje, zda použitá VPN subsíť nekoliduje s rozsahy IP adres na vzdáleném konci tunelu.
   Je-li po spuštění VPN serveru (tzn. po stisknutí tlačítka *Použít* v sekci *Rozhraní*) hlášena kolize rozsahu adres pro VPN s lokální sítí, pak je třeba nastavit VPN subsíť ručně. Zvolte subsíť, která není použita v žádné z propojovaných lokálních sítí. VPN subsítě na každém konci tunelu musí být různé (bude tedy třeba vybrat dvě volné subsítě).
3. VPN klientům lze přidělovat statické IP adresy na základě uživatelského jména, kterým se klient přihlašuje. Podrobnosti viz kapitola 15.1.

SSL certifikát

Informace o aktuálním certifikátu VPN serveru. Tento certifikát slouží k ověření identity serveru při vytváření VPN tunelu (podrobnosti viz kapitola 23.3). VPN server ve *WinRoute* používá standardní SSL certifikát (podobně jako např. zabezpečené WWW rozhraní).
Při definici VPN tunelu je třeba předat otisk certifikátu lokálního konce tunelu vzdálenému konci a naopak (pro vzájemné ověření identity — viz kapitola 23.3).

Tip

Otisk certifikátu lze označit myší, zkopírovat do schránky a vložit do textového souboru, e-mailové zprávy apod.

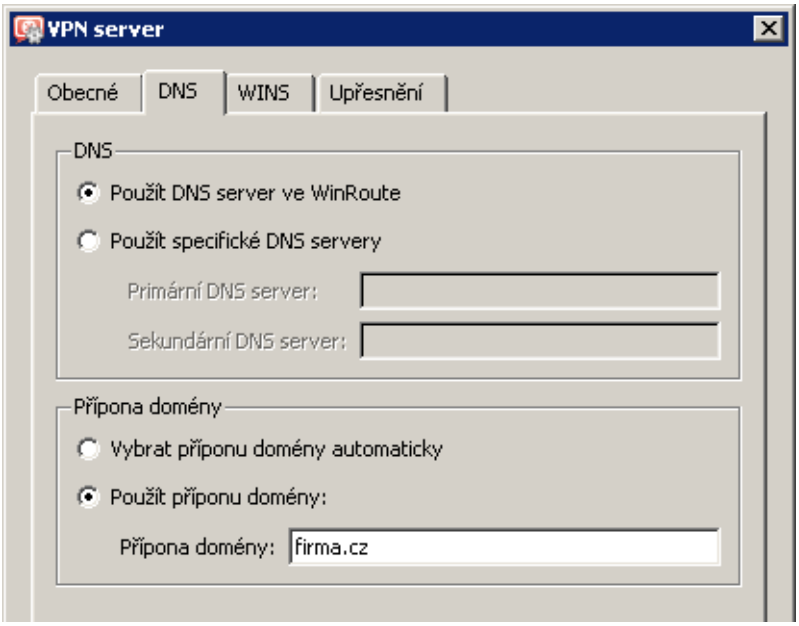
Tlačítko *Změnit SSL certifikát* otevírá dialog pro nastavení certifikátu VPN serveru. Pro VPN server můžete vytvořit vlastní certifikát (podepsaný sám sebou) nebo importovat certifikát vydaný důvěryhodnou certifikační autoritou. Vytvořený certifikát se uloží do podadresáře `sslcert` instalačního adresáře *WinRoute* pod názvem `vpn.crt` a příslušný privátní klíč pod názvem `vpn.key`.
Postupy vytvoření a importu SSL certifikátu jsou podrobně popsány v kapitole 11.1.
Poznámka: Pokud již máte certifikát vystavený certifikační autoritou pro váš server (např. pro zabezpečené WWW rozhraní), můžete jej rovněž použít pro VPN server — není třeba žádat o vystavení nového certifikátu.

Konfigurace DNS pro VPN klienty

Aby mohli VPN klienti přistupovat na počítače v lokální síti jejich jmény, musejí mít k dispozici alespoň jeden DNS server z lokální sítě.

VPN server ve *WinRoute* nabízí tyto možnosti konfigurace DNS serverů:

- *DNS server ve WinRoute* — VPN klientům bude jako primární DNS server nastavena IP adresa příslušného rozhraní počítače s *WinRoute* — VPN klienti budou používat



Obrázek 23.4 Nastavení VPN serveru — specifikace DNS serverů pro VPN klienty

modul *DNS* (viz kapitola 8.1). Toto je výchozí volba, pokud je modul *DNS* ve *WinRoute* povolen.
Pokud je modul *DNS* používán jako DNS server pro počítače v lokální síti, doporučujeme jej používat i pro VPN klienty. Modul *DNS* zajišťuje nejrychlejší možnou odezvu na DNS dotazy klientů a zároveň je vyloučena případná nekonzistence v DNS záznamech.

- *Specifické DNS servery* — VPN klientům bude nastaven zadaný primární, případně také sekundární DNS server.
  Tuto volbu použijte, pokud je v lokální síti používán jiný DNS server než modul *DNS* ve *WinRoute*.

VPN klientům je rovněž přidělována přípona DNS domény. Přípona domény určuje lokální doménu. Má-li VPN klient příponu domény shodnou s lokální doménou v síti, do které se připojuje, může se na počítače v této síti odkazovat jejich jmény (např. `server`). V opačném případě musí uvádět celé jméno počítače včetně domény (např. `server.firma.local`).

Přípona DNS může být rovněž zjištěna automaticky nebo nastavena ručně:

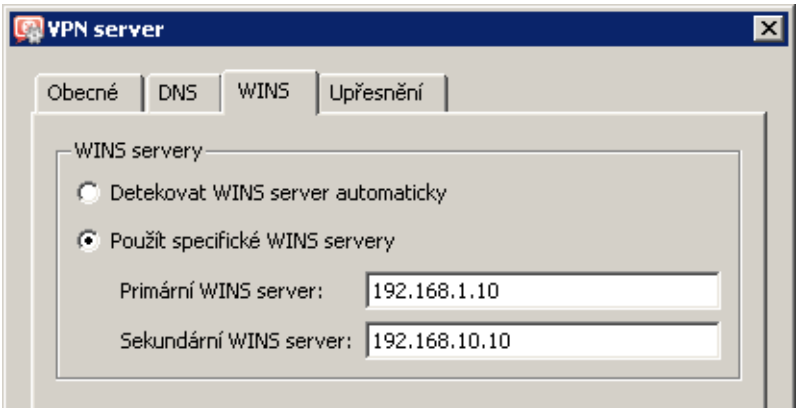
- Automatické nastavení přípony lze použít v případě, pokud je počítač členem domény *Active Directory* a/nebo pokud jsou uživatelé firewallu ověřováni v této doméně (viz kapitola 15.1).
- DNS doménu je potřeba specifikovat, pokud se jedná o doménu *Windows NT* nebo síť bez domény, případně v situaci, kdy chceme VPN klientům nastavit jinou příponu domény (např. v případě mapování více domén *Active Directory*).

Poznámka: DNS servery přidělené VPN serverem budou na počítači klienta použity jako primární, resp. sekundární DNS server. Z toho vyplývá, že *všechny* DNS dotazy z počítače klienta

budou posílány na tyto servery. Ve většině případů však toto „přesměrování“ nemá žádný vedlejší efekt. Po ukončení VPN spojení bude obnovena původní konfigurace DNS.

Konfigurace WINS pro VPN klienty

Služba WINS zajišťuje převod jmen počítačů na IP adresy v síti *Microsoft Windows*. Přidělení adresy WINS serveru umožní VPN klientům procházet počítače v lokální síti (*Okolní počítače / Místa v síti*).



Obrázek 23.5 Nastavení VPN serveru — specifikace WINS serverů pro VPN klienty

WinRoute může WINS server(y) detekovat automaticky (z konfigurace počítače, na kterém je nainstalován) nebo použít zadané adresy primárního, případně sekundárního WINS serveru. Automatickou konfiguraci lze použít vždy, pokud máme jistotu, že jsou WINS servery na počítači s *WinRoute* nastaveny správně.

Upřesňující nastavení

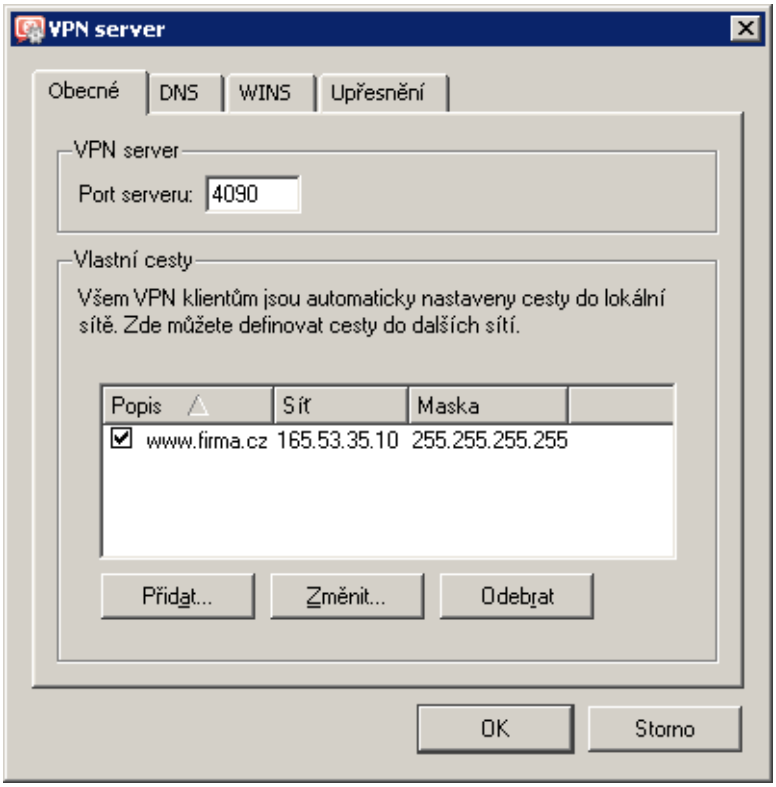
Port serveru

Port, na kterém VPN server čeká na příchozí spojení (používá se protokol TCP i UDP). Výchozí port je 4090 (za normálních okolností není třeba číslo portu měnit).
Poznámka:

1. Pokud je již VPN server spuštěn, pak při změně portu dojde k odpojení všech připojených VPN klientů.
2. Nelze-li spustit VPN server na zadaném portu (port je využíván jinou službou), pak se po stisknutí tlačítka *Použít* zapíše do záznamu *Error* (viz kapitola 22.8) následující chybové hlášení:

```
(4103:10048) Socket error: Unable to bind socket
for service to port 4090.

(5002) Failed to start service "VPN"
bound to address 192.168.1.1.
```



Obrázek 23.6 Nastavení VPN serveru — port serveru a vlastní cesty pro VPN klienty

Pokud si nejste zcela jisti, zda je zadaný port skutečně volný, zkontrolujte po spuštění VPN serveru záznam *Error*, zda se v něm takovéto hlášení neobjevilo.

Vlastní cesty

Tato sekce dialogu umožňuje specifikovat další sítě, do kterých bude VPN klientovi nastavena cesta (standardně jsou klientům nastaveny cesty do všech subsítí lokálních na straně VPN serveru— viz kapitola 23.4).

Tip

Použitím masky subsítě `255.255.255.255` definujeme cestu ke konkrétnímu počítači. Toho lze využít např. pro přidání cesty k počítači umístěnému v demilitarizované zóně na straně VPN serveru.

23.2 Nastavení pro VPN klienty

Připojování vzdálených klientů do lokální sítě zabezpečeným šifrovaným kanálem je možné za následujících podmínek:

- Na vzdáleném počítači musí být nainstalována aplikace *Kerio VPN Client* (podrobnosti viz samostatný manuál *Kerio VPN Client — Příručka uživatele*).
- Příslušný uživatel (jehož uživatelský účet bude použit pro ověření v aplikaci *Kerio VPN Client*) musí mít právo připojovat se k VPN serveru ve *WinRoute* (viz kapitola 15.1).
- Připojení k VPN serveru z Internetu a komunikace mezi VPN klienty musí být povoleny komunikačními pravidly.

Poznámka: Vzdálení VPN klienti připojující se k *WinRoute* se započítávají do celkového počtu uživatelů při kontrole licence (viz kapitola 4, resp. 4.6). Tuto skutečnost je třeba vzít v úvahu při rozhodování, jaká licence bude zakoupena, případně zakoupit k existující licenci rozšíření (add-on) na vyšší počet uživatelů.

Tip:
Přehled VPN klientů aktuálně připojených k firewallu lze zobrazit v *Administration Console* v sekci *Stav* → *VPN klienti*. Podrobnosti viz kapitola 19.3.

Základní nastavení komunikačních pravidel pro VPN klienty

Jméno	Zdroj	Cíl	Služba	Akce
Služba Kerio VPN	Internet	Firewall	Kerio VPN	✓
Lokální komunikace	Firewall Všichni VPN klienti Důvěryhodné / lokální	Firewall Všichni VPN klienti Důvěryhodné / lokální	Libovolný	✓

Obrázek 23.7 Obecná komunikační pravidla pro VPN klienty

- První pravidlo povoluje připojení k VPN serveru ve *WinRoute* z Internetu.
  Chceme-li omezit přístup k VPN serveru pouze z určitých IP adres, upravíme příslušným způsobem položku *Zdroj*.
  Služba *Kerio VPN* je standardně definována pro protokoly TCP a UDP, port 4090. Pokud je VPN server spuštěn na jiném portu, pak je třeba upravit definici této služby.
- Druhé pravidlo povoluje komunikaci mezi firewallem, lokální sítí a VPN klienty.

S takto nastavenými komunikačními pravidly mají všichni VPN klienti neomezený přístup do lokální sítě a naopak (ze všech počítačů v lokální síti lze komunikovat se všemi připojenými VPN klienty). Chceme-li přístup omezit, je třeba pro VPN klienty definovat samostatná pravidla. Některé možnosti nastavení pravidel pro omezení komunikace v rámci *Kerio VPN* jsou popsány v příkladu v kapitole 23.5.

Poznámka:

1. Při vytváření komunikačních pravidel pomocí *Průvodce komunikačními pravidly* mohou být výše popsaná pravidla vytvořena automaticky (včetně zařazení VPN klientů do položek *Zdroj* a *Cíl*). Pro vytvoření těchto pravidel zvolíme *Ano, chci používat Kerio VPN* v 5. kroku průvodce. Podrobnosti viz kapitola 7.1.

2. Pro přístup do Internetu používá každý VPN klient své stávající internetové připojení. VPN klienti nemohou přistupovat přes *WinRoute* do Internetu (klientům nelze změnit nastavení výchozí brány).

3. Podrobné informace o definici komunikačních pravidel naleznete v kapitole 7.

23.3 Propojení dvou privátních sítí přes Internet (VPN tunel)

Pro vytvoření zabezpečeného šifrovaného tunelu mezi lokální a vzdálenou sítí přes Internet (dále jen „VPN tunel“) musí být v obou sítích nainstalován *WinRoute* včetně podpory VPN (v typické instalaci je podpora VPN obsažena).

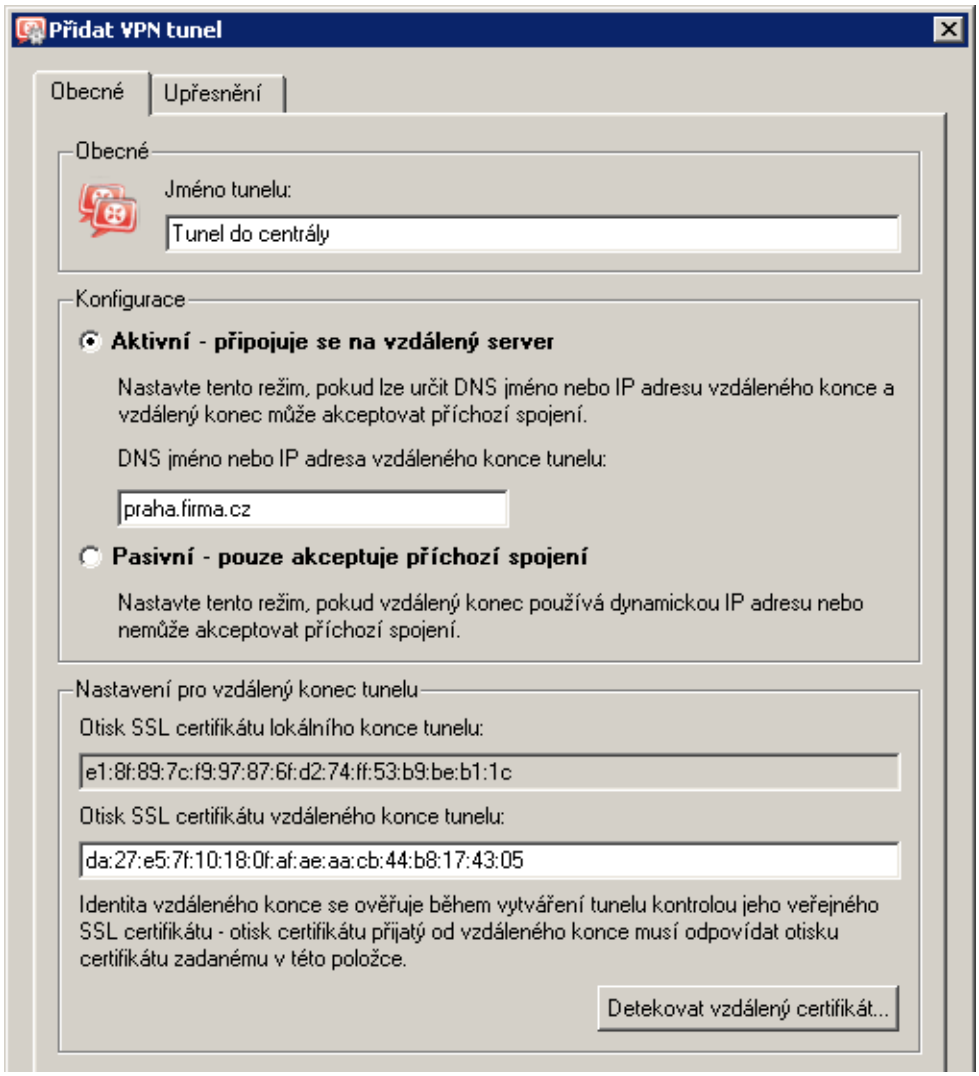
Poznámka: Každá instalace *WinRoute* vyžaduje samostatnou licenci (viz kapitola 4).

Nastavení VPN serverů

Nejprve je třeba na obou stranách (koncích tunelu) povolit a nastavit VPN server. Podrobnosti o konfiguraci VPN serveru naleznete v kapitole 23.1.

Definice tunelu na vzdálený server

Na každé straně musí být definován VPN tunel na protější server. Volbou *Přidat* → *VPN tunel* otevřeme dialog pro vytvoření nového tunelu.



Obrázek 23.8 Konfigurace VPN tunelu

Jméno tunelu

Každému VPN tunelu musí být přiřazeno jednoznačné jméno. Pod tímto jménem se tunel zobrazuje v tabulce rozhraní, v komunikačních pravidlech (viz kapitola 7.3) a ve statistikách rozhraní (viz kapitola 20.2).

Konfigurace

Nastavení režimu lokálního konce tunelu:

- *Aktivní* — tento konec tunelu bude sám navazovat spojení na vzdálený VPN server (po vytvoření tunelu, po povolení tunelu nebo po výpadku spojení).
  V položce *DNS jméno nebo IP adresa vzdáleného konce tunelu* musí být uveden vzdálený VPN server. Používá-li VPN server jiný port než `4090`, musí být za dvojtečkou uvedeno příslušné číslo portu (např. `server.firma.cz:4100` nebo `65.35.55.20:9000`).
  Aktivní režim může být použit, jestliže lze určit IP adresu nebo DNS jméno vzdáleného konce tunelu a vzdálený konec může akceptovat příchozí spojení (tzn. komunikace na vzdálené straně není blokována firewallem).
- *Pasivní* — tento konec tunelu bude pouze akceptovat příchozí spojení od vzdáleného (aktivního) konce tunelu.
  Pasivní režim má smysl pouze v případě, že lokální konec tunelu má pevnou IP adresu a může akceptovat příchozí spojení.

Alespoň jeden konec každého VPN tunelu musí být nastaven do aktivního režimu (pasivní konec nemůže navazovat spojení).

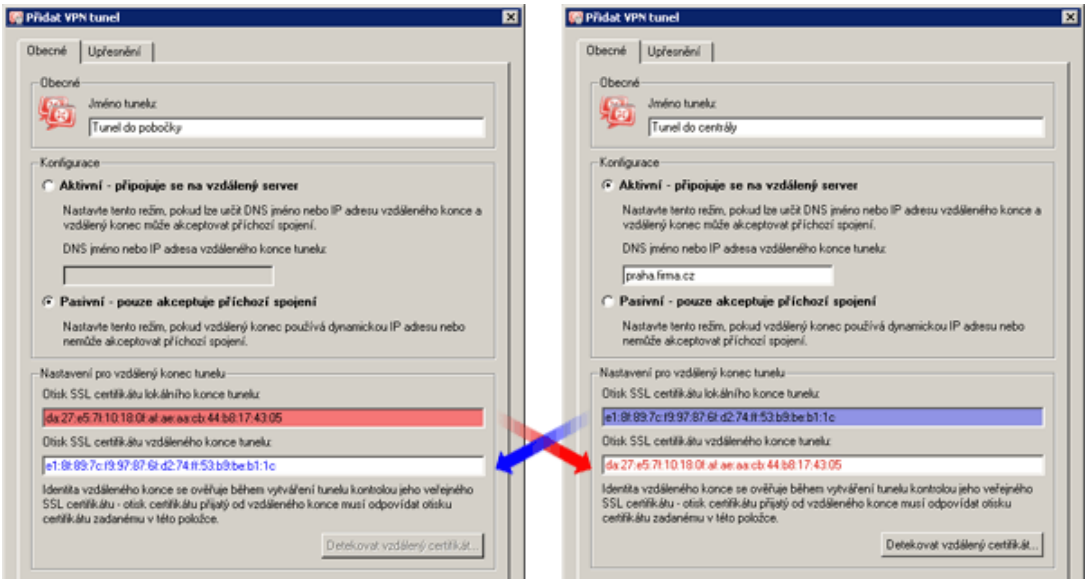
Nastavení pro vzdálený konec tunelu

Při vytváření VPN tunelu se ověřuje identita vzdáleného konce kontrolou otisku jeho SSL certifikátu. Nesouhlasí-li otisk certifikátu přijatého ze vzdáleného konce s otiskem uvedeným v nastavení tunelu, spojení bude odmítnuto.

V sekci *Nastavení pro vzdálený konec tunelu* je uveden otisk certifikátu lokálního konce tunelu a pod ním položka pro otisk certifikátu vzdáleného konce. Do této položky je třeba zadat otisk certifikátu VPN serveru na protější straně a naopak (při konfiguraci tunelu na protější straně musí být zadán otisk certifikátu tohoto VPN serveru).

Je-li lokální konec tunelu nastaven do aktivního režimu, pak lze stisknutím tlačítka *Detekovat vzdálený certifikát* načíst certifikát vzdáleného konce a jeho otisk nastavit do příslušné položky. Pasivní konec tunelu nemůže vzdálený certifikát detekovat.

Tento způsob nastavení otisku certifikátu je však méně bezpečný — může dojít k podvržení certifikátu. Pokud bude v konfiguraci tunelu nastaven otisk podvrženého certifikátu, pak bude možné vytvořit tunel s útočníkem vydávajícím se za protější stranu. Naopak platný certifikát protější strany nebude akceptován. Je-li to možné, doporučujeme nastavit otisky certifikátů ručně.



Obrázek 23.9 VPN tunel — otisky certifikátů

Nastavení DNS

Aby bylo možné přistupovat na počítače ve vzdálené síti (tzn. na protější straně tunelu) jejich DNS jmény, je třeba správně nastavit DNS na obou stranách tunelu. Jedním z možných řešení je přidat do DNS na každé straně tunelu záznamy o počítačích na protější straně. Tento přístup je však administrativně náročný a neflexibilní.

Bude-li na obou stranách tunelu jako DNS server použit modul *DNS* ve *WinRoute*, můžeme v pravidlech pro předávání DNS dotazů (viz kapitola 8.1) jednoduše nastavit předávání dotazů na jména v příslušné doméně modulu *DNS* na protější straně tunelu. Podmínkou je použití jiné DNS domény (resp. subdomény) na každé straně tunelu.

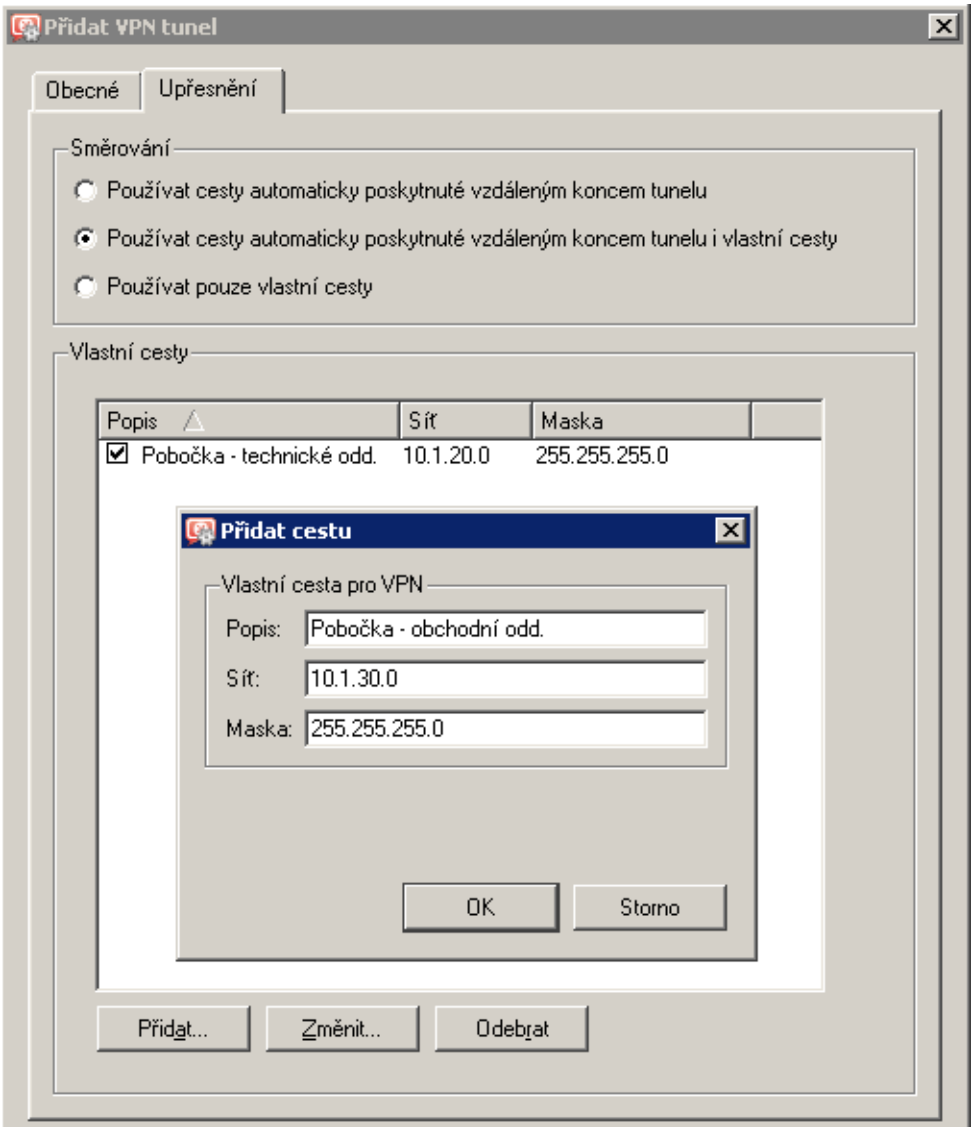
Poznámka: Pro správné předávání DNS dotazů vyslaných z počítače s *WinRoute* (na kterékoliv straně VPN tunelu) je třeba, aby tyto dotazy také zpracovával modul *DNS*. Toho docílíme tak, že na každém firewallu nastavím na rozhraní připojeném do lokální sítě DNS server „sám na sebe“ (tzn. jako adresu DNS serveru použijeme IP adresu daného rozhraní).

Postup konfigurace DNS je podrobně popsán na příkladu v kapitole 23.5.

Nastavení směrování

Záložka *Upřesnění* umožňuje nastavit, zda a jakým způsobem budou do lokální směrovací tabulky přidávány cesty poskytnuté vzdáleným koncem VPN tunelu, a případně definovat vlastní cesty do vzdálených sítí.

Problematika směrování v rámci *Kerio VPN* je podrobně popsána v kapitole 23.4.



Obrázek 23.10 Nastavení směrování pro VPN tunel

Navázání spojení

Aktivní konec tunelu se snaží automaticky navázat spojení vždy, když detekuje, že tunel je odpojen (k prvnímu pokusu o navázání spojení dojde bezprostředně po definici tunelu a stisknutí tlačítka *Použít* v sekci *Konfigurace* → *Rozhraní*, resp. po povolení příslušné komunikace — viz dále).

VPN tunel lze deaktivovat tlačítkem *Zakázat*. Při deaktivaci tunelu by vždy měly být zakázány oba jeho konce.

Poznámka: VPN tunel se udržuje navázaný (zasíláním speciálních paketů v pravidelném časovém intervalu), i pokud se nepřenášejí žádná data. Toto je ochrana proti ukončení spojení firewallem nebo jiným síťovým prvkem na cestě mezi koncovými body tunelu.

Komunikační pravidla pro VPN tunel

Po vytvoření VPN tunelu je třeba povolit komunikaci mezi lokální sítí a sítí připojenou tímto tunelem a povolit odchozí spojení pro službu *Kerio VPN* z firewallu do Internetu. Jsou-li vytvořena základní komunikační pravidla pomocí průvodce (viz kapitola 23.2), stačí přidat příslušný VPN tunel do pravidla *Lokální komunikace* a do pravidla *Komunikace firewallu* přidat službu *Kerio VPN*. Výsledná komunikační pravidla jsou uvedena na obrázku 23.11.

Jméno	Zdroj	Cíl	Služba	Akce
Služba Kerio VPN	Internet	Firewall	Kerio VPN	✓
Lokální komunikace	Firewall Všichni VPN klienti Tunel do pobočky Důvěryhodné / lokální	Firewall Všichni VPN klienti Tunel do pobočky Důvěryhodné / lokální	Libovolný	✓
Komunikace firewallu	Firewall	Libovolný	DNS FTP HTTP HTTPS IMAP Kerio VPN POP3 SMTP Telnet	✓

Obrázek 23.11 Komunikační pravidla pro VPN tunel

Poznámka:

1. V příkladech v tomto manuálu budeme pro jednoduchost uvažovat, že pravidlo *Komunikace firewallu* povoluje přístup firewallu k libovolné službě (viz obrázek 23.12). Pak samozřejmě není nutné službu *Kerio VPN* do tohoto pravidla přidávat.

Jméno	Zdroj	Cíl	Služba	Akce
Služba Kerio VPN	Internet	Firewall	Kerio VPN	✓
Lokální komunikace	Firewall Všichni VPN klienti Tunel do pobočky Důvěryhodné / lokální	Firewall Všichni VPN klienti Tunel do pobočky Důvěryhodné / lokální	Libovolný	✓
Komunikace firewallu	Firewall	Libovolný	Libovolný	✓

Obrázek 23.12 Obecná komunikační pravidla pro VPN tunel

2. Takto nastavená komunikační pravidla povolují komunikaci mezi lokální sítí, vzdálenou sítí a všemi VPN klienty bez omezení. Chceme-li omezit přístup, je třeba definovat několik samostatných pravidel (pro lokální komunikaci, VPN klienty, VPN tunel atd.). Některé možnosti nastavení komunikačních pravidel jsou uvedeny v příkladu v kapitole 23.5.

23.4 Výměna směrovacích informací

Mezi koncovými body VPN tunelu, resp. z VPN serverem a VPN klientem probíhá automatická výměna směrovacích informací (tj. údajů o cestách do lokálních subsítí). Směrovací tabulky na obou stranách jsou tak stále udržovány v aktuálním stavu.

Možnosti konfigurace směrování

Za normálních okolností není třeba nastavovat žádné vlastní cesty — příslušné cesty budou do směrovacích tabulek přidány automaticky, a to i při změnách konfigurace sítě na některém konci tunelu (resp. na straně VPN serveru). Pokud však směrovací tabulka na některém konci VPN tunelu obsahuje nesprávné cesty (např. chybou správce), pak jsou tyto cesty rovněž předávány. Komunikace s některými vzdálenými subsítěmi nebude možná a VPN tunelem bude zbytečně přenášeno velké množství řídicích zpráv.

Obdobná situace může nastat v případě VPN klienta připojujícího se k VPN serveru ve *WinRoute*.

Pro ošetření uvedených situací lze v dialogu pro definici VPN tunelu (viz kapitola 23.3), resp. pro nastavení VPN serveru (viz kapitola 23.1) nastavit, jaké směrovací informace budou používány, a definovat vlastní cesty.

V *Kerio VPN* mohou být směrovací informace předávány jedním z těchto způsobů:

- *Automaticky poskytnuté cesty* (výchozí nastavení) — cesty do vzdálených sítí se nastavují automaticky dle informací poskytnutých protějším koncem tunelu. V tomto případě není třeba nic konfigurovat, může však docházet k problémům s chybnými cestami (viz výše).
- *Automaticky poskytnuté cesty i vlastní cesty* — automaticky nastavené cesty jsou doplněny cestami definovanými ručně na lokálním konci tunelu. V případě konfliktu mají přednost vlastní cesty. Takto lze snadno ošetřit situaci, kdy vzdálený konec tunelu poskytuje jednu nebo více nesprávných cest.
- *Pouze vlastní cesty* — všechny cesty do vzdálených sítí musí být nastaveny ručně na lokálním konci tunelu. Tento způsob eliminuje přidání chybných cest poskytnutých vzdáleným koncem tunelu do lokální směrovací tabulky, je však značně administrativně náročný (při každé změně v konfiguraci vzdálené sítě je třeba upravit nastavení vlastních cest).

Automaticky předávané cesty

Pokud nejsou definovány žádné vlastní cesty, platí pro výměnu směrovacích informací platí následující pravidla:

- nepředává se výchozí cesta a cesta do sítě s výchozí bránou (vzdálenému konci tunelu, resp. VPN klientovi nelze změnit výchozí bránu),
- nepředávají se cesty do subsítí, které se nacházejí na obou stranách tunelu (z principu není možné provádět směrování lokální a vzdálenou sítí se stejným rozsahem IP adres),
- všechny ostatní cesty jsou předávány (tzn. cesty do lokálních subsítí včetně subsítí na vzdálených koncích ostatních VPN tunelů s výjimkou předchozího bodu, všechny ostatní VPN a všichni VPN klienti).

Poznámka: Z výše uvedených pravidel vyplývá, že při vytvoření dvou VPN tunelů mohou obě vzdálené sítě komunikovat mezi sebou. Komunikační pravidla mohou být přitom nastavena tak, že ani jedna ze vzdálených sítí nebude moci přistupovat do lokální sítě.

Aktualizace směrovacích tabulek

Směrovací informace jsou předávány vždy:

- při navázání VPN tunelu nebo připojení VPN klienta k serveru,
- při změně směrovací tabulky na některé straně tunelu (resp. na VPN serveru),
- periodicky v intervalu 10 minut. Čas je vždy měřen od poslední aktualizace (bez ohledu na to, z jakého důvodu byla provedena).

23.5 Příklad konfigurace Kerio VPN: firma s pobočkou

V této kapitole uvádíme postup vytvoření zabezpečeného šifrovaného tunelu mezi dvěma privátními sítěmi pomocí *Kerio VPN*.

Uvedený příklad lze snadno modifikovat a přizpůsobit konkrétním konfiguracím sítí, které mají být VPN tunely propojeny. Popsaný způsob konfigurace lze použít v případech, kdy vytvořením VPN tunelů nevzniknou redundantní cesty (tj. více různých cest mezi jednotlivými privátními sítěmi). Popis konfigurace VPN s redundantními cestami (typické pro firmu se dvěma a více pobočkami) naleznete v kapitole 23.6.

Poznámka: Tento příklad řeší složitější model VPN s nastavením omezení přístupu pro jednotlivé lokální sítě a VPN klienty. Jednoduchý příklad základního nastavení VPN naleznete v manuálu *Kerio WinRoute Firewall — Konfigurace krok za krokem*.

Zadání

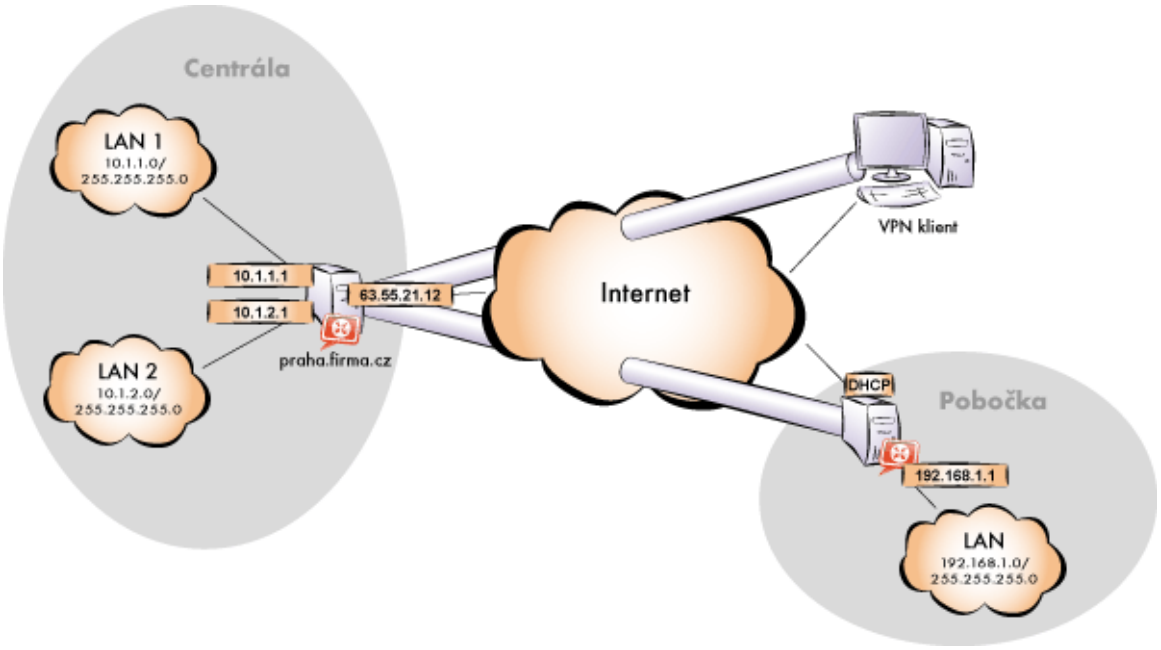
Fiktivní firma má centrálu v Praze a pobočku v Plzni. Lokální sítě centrály a pobočky mají být propojeny VPN tunelem za použití *Kerio VPN*. Do sítě centrály má být umožněn přístup VPN klientům.

Server (výchozí brána) centrály má pevnou veřejnou IP adresu `63.55.21.12` (DNS jméno `praha.firma.cz`), server pobočky má dynamickou veřejnou IP adresu přidělovanou protokolem DHCP.

Lokální síť centrály tvoří dvě subsítě `LAN 1` a `LAN 2`. Centrála používá DNS doménu `firma.cz`.

Síť pobočky firmy je tvořena pouze jednou subsítí (označena `LAN`). Pobočka používá DNS subdoménu `pobocka.firma.cz`.

Schéma uvažovaných sítí včetně IP adres a požadovaného VPN tunelu je znázorněno na obrázku 23.13.



Obrázek 23.13 Příklad — propojení centrály a pobočky firmy VPN tunelem s možností připojení VPN klientů

Předpokládejme, že obě sítě jsou již zapojeny a nastaveny podle tohoto schématu a internetové připojení na obou stranách je funkční.

Komunikace mezi sítí centrály a pobočky a VPN klienty má být omezena podle následujících pravidel:

1. VPN klienti smí přistupovat do sítě `LAN 1` v centrále a do sítě pobočky.
2. Ze všech sítí je zakázán přístup na VPN klienty.
3. Z pobočky je povolen přístup pouze do sítě `LAN 1`, a to pouze ke službám *WWW*, *FTP* a *Microsoft SQL*.
4. Z centrály je povolen přístup do pobočky bez omezení.
5. Do sítě `LAN 2` je zakázán přístup ze sítě pobočky i VPN klientům.

Obecný postup

V obou lokálních sítích (tj. v centrále i v pobočce firmy) je třeba provést tyto kroky:

1. Na výchozí bráně sítě musí být nainstalován *WinRoute* verze `6.0.0` nebo vyšší (starší verze neobsahují proprietární VPN řešení *Kerio VPN*).

   Poznámka: Pro *každou* instalaci *WinRoute* je potřeba samostatná licence pro příslušný počet uživatelů! Podrobnosti viz kapitola 4.

2. Nastavíme a otestujeme přístup z lokální sítě do Internetu. Počítače v lokální síti musí mít jako výchozí bránu a upřednostňovaný (primární) DNS server nastavenu IP adresu počítače s *WinRoute*.

   Jedná-li se o novou (čistou) instalaci *WinRoute*, můžeme využít průvodce komunikačními pravidly (viz kapitola 7.1).

   Podrobný popis základní konfigurace *WinRoute* a lokální sítě je uveden v samostatném manuálu *Kerio WinRoute Firewall — konfigurace krok za krokem*.

3. V konfiguraci modulu *DNS* nastavíme pravidla pro předávání DNS dotazů pro doménu ve vzdálené síti. Tím umožníme přístup na počítače ve vzdálené síti jejich DNS jmény (v opačném případě by bylo nutné zadávat vzdálené počítače IP adresami).

   Pro správné předávání DNS dotazů z počítače s *WinRoute* musíme na tomto počítači nastavit primární DNS server „sám na sebe“ (tzn. použít IP adresu některého síťového rozhraní tohoto počítače). Jako sekundární DNS server pak musí být specifikován server, na který budou předávány DNS dotazy do ostatních domén (typicky DNS server poskytovatele internetového připojení).

   Poznámka: Pro správnou funkci DNS musí DNS databáze obsahovat záznamy o počítačích v příslušné lokální síti. Toho lze docílit zapsáním IP adres a DNS jmen lokálních počítačů do souboru `hosts` (v případě statických IP adres) nebo nastavením spolupráce modulu *DNS* s DHCP serverem (v případě dynamicky přidělovaných IP adres). Podrobnosti viz kapitola 8.1.

4. V sekci *Rozhraní* povolíme VPN server, případně nastavíme jeho SSL certifikát. Poznamenáme si otisk certifikátu serveru — budeme jej potřebovat při konfiguraci vzdáleného konce VPN tunelu .

   Zkontrolujeme, zda automaticky vybraná VPN subsíť nekoliduje s žádnou lokální subsítí v centrále ani v pobočce; případně vybereme jinou volnou subsíť.

5. Definujeme VPN tunel do vzdálené sítě. Pasivní konec tunelu musí být vytvořen na serveru, který má pevnou veřejnou IP adresu (tj. na serveru centrály). Na serveru s dynamickou IP adresou lze vytvářet pouze aktivní konce VPN tunelů.

   Je-li protější konec tunelu již definován, zkontrolujeme, zda došlo ke spojení (navázání) tunelu. V případě neúspěchu prohlédneme záznam *Error*, zkontrolujeme otisky certifikátů a prověříme dostupnost vzdáleného serveru.

6. V komunikačních pravidlech povolíme komunikaci mezi lokální sítí, vzdálenou sítí a VPN klienty a nastavíme požadovaná omezení přístupu. V uvažované konfiguraci sítě lze nastavit všechna požadovaná omezení na serveru centrály, proto na serveru pobočky pouze povolíme komunikaci mezi lokální sítí a VPN tunelem.

7. Z každé lokální sítě otestujeme dostupnost počítačů ve vzdálené síti. Pro tento test můžeme použít systémové příkazy `ping` a `tracert`. Ověříme dostupnost počítače ve vzdálené síti zadaného jednak IP adresou, jednak DNS jménem.

   Nedostaneme-li odezvu při zadání vzdáleného počítače IP adresou, je třeba hledat chybu v nastavení komunikačních pravidel, případně prověřit, zda nenastala kolize subsítí (stejná subsíť na obou stranách tunelu).

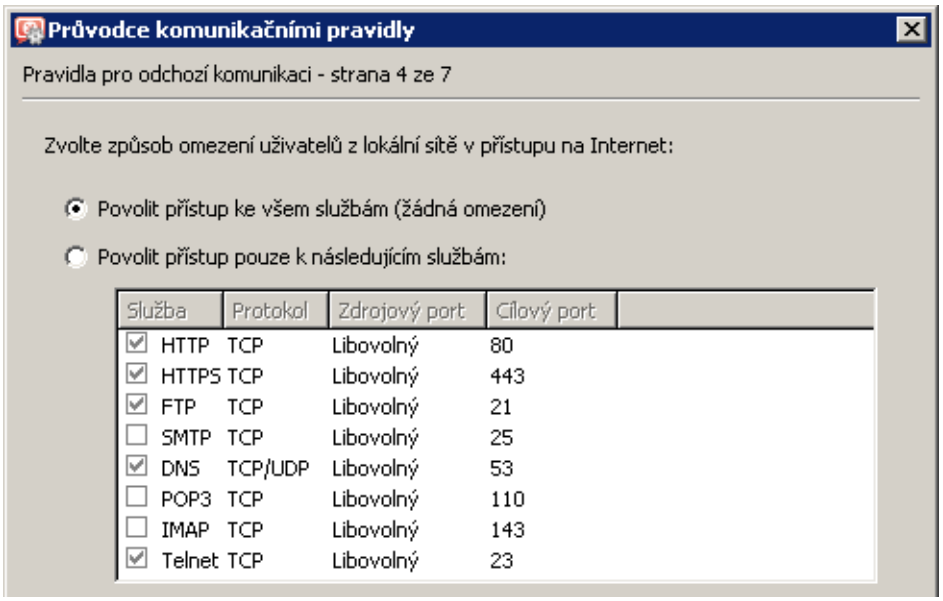
   Je-li test při zadání počítače IP adresou úspěšný, ale při zadání počítače DNS jménem je hlášena chyba (*Neznámý hostitel*), pak je třeba prověřit konfiguraci DNS.

Následující sekce podrobně popisují konfiguraci *Kerio VPN* v centrále a v pobočkách firmy.

Konfigurace v centrále firmy

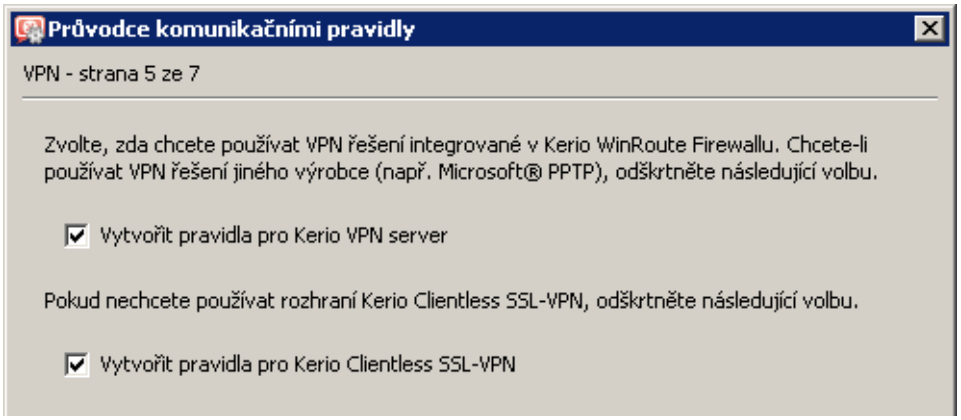
1. Na výchozí bránu sítě centrály (dále jen „server“) nainstalujeme *WinRoute* (verze `6.0.0` nebo vyšší).

2. Ve *WinRoute* nastavíme základní komunikační pravidla pomocí *Průvodce komunikačními pravidly* (viz kapitola 7.1). Pro jednoduchost předpokládejme, že nebudeme omezovat přístup z lokální sítě do Internetu, tzn. ve 4. kroku průvodce povolíme přístup ke všem službám.



Obrázek 23.14 Centrála — přístup z lokální sítě do Internetu bez omezení

V 5. kroku průvodce zvolíme *Vytvořit pravidla pro Kerio VPN server*. Na nastavení volby *Vytvořit pravidla pro Kerio Clientless SSL-VPN* nezáleží (tento příklad se nezabývá rozhraním *Clientless SSL-VPN*).



Obrázek 23.15 Centrála — vytvoření výchozích komunikačních pravidel pro Kerio VPN

Tím dojde k vytvoření pravidel pro připojení k VPN serveru a pro komunikaci VPN klientů s lokální sítí, resp. firewallem.

Jméno	Zdroj	Cíl	Služba	Akce
Služba Kerio VPN	Internet	Firewall	Kerio VPN	✓
Lokální komunikace	Firewall Všichni VPN klienti Důvěryhodné / lokální	Firewall Všichni VPN klienti Důvěryhodné / lokální	Libovolný	✓
Komunikace firewallu	Firewall	Libovolný	Libovolný	✓

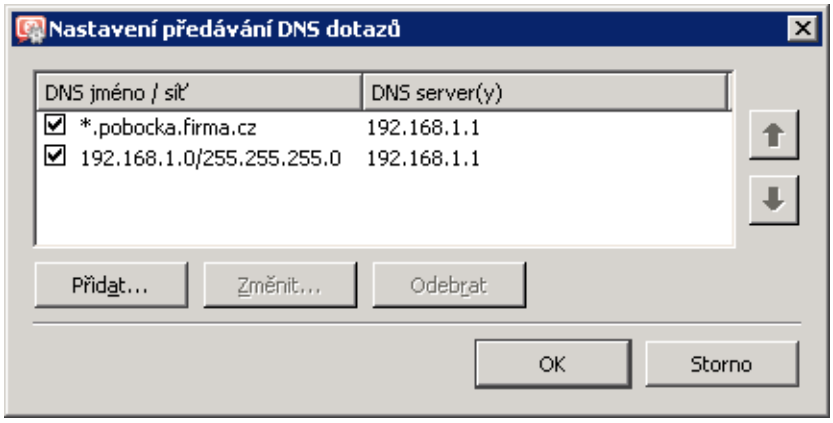
Obrázek 23.16 Centrála — výchozí komunikační pravidla pro Kerio VPN

Po vytvoření VPN tunelu tato pravidla upravíme dle požadavků na omezení přístupu (viz bod 6.).

Poznámka: Z důvodu jednoduchosti a přehlednosti jsou v tomto příkladu uvedena pouze komunikační pravidla relevantní pro konfiguraci *Kerio VPN*.

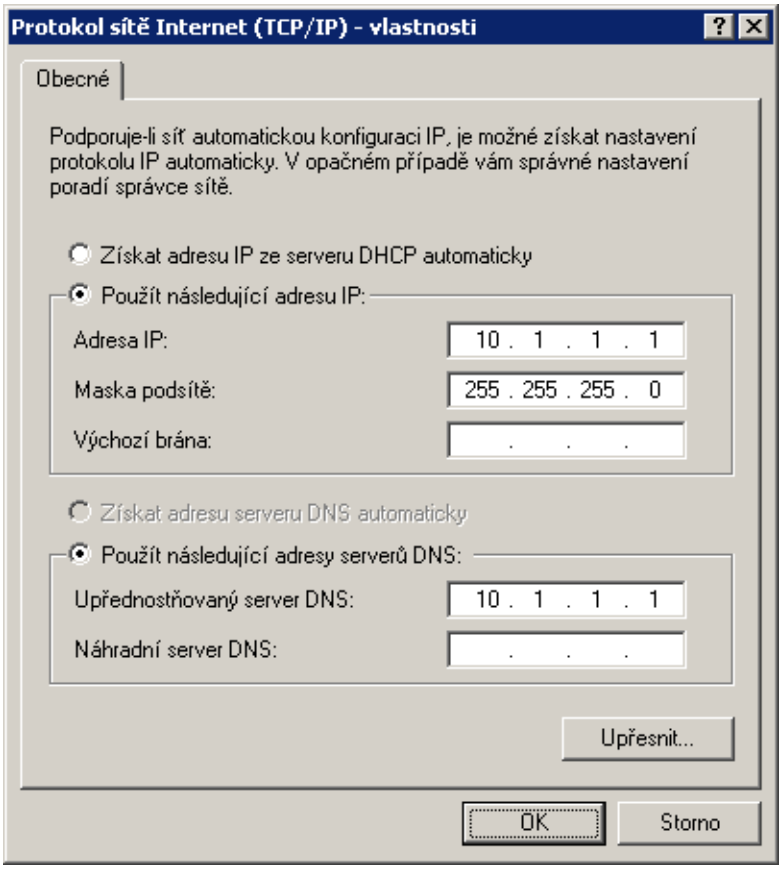
3. Nastavíme DNS (resp. upravíme nastavení DNS):

   - V konfiguraci modulu *DNS* ve *WinRoute* povolíme službu *DNS forwarder* (předávání DNS dotazů jiným serverům).
   - Zapneme volbu *Použít nastavení pro předávání DNS dotazů* a definujeme pravidla pro jména v doméně `pobocka.firma.cz`. Jako DNS server pro předávání dotazů uvedeme IP adresu vnitřního rozhraní počítače s *WinRoute* na protější straně tunelu (tj. rozhraní připojeného do lokální sítě na protější straně).



Obrázek 23.17 Centrála — nastavení předávání DNS dotazů

- Na rozhraní počítače s *WinRoute* připojeném do lokální sítě *LAN 1* nastavíme jako upřednostňovaný (primární) DNS server IP adresu tohoto rozhraní (tj. `10.1.1.1`). Na rozhraní připojeném do sítě *LAN 2* již DNS server nastavovat nemusíme — konfigurace DNS platí globálně pro celý operační systém.



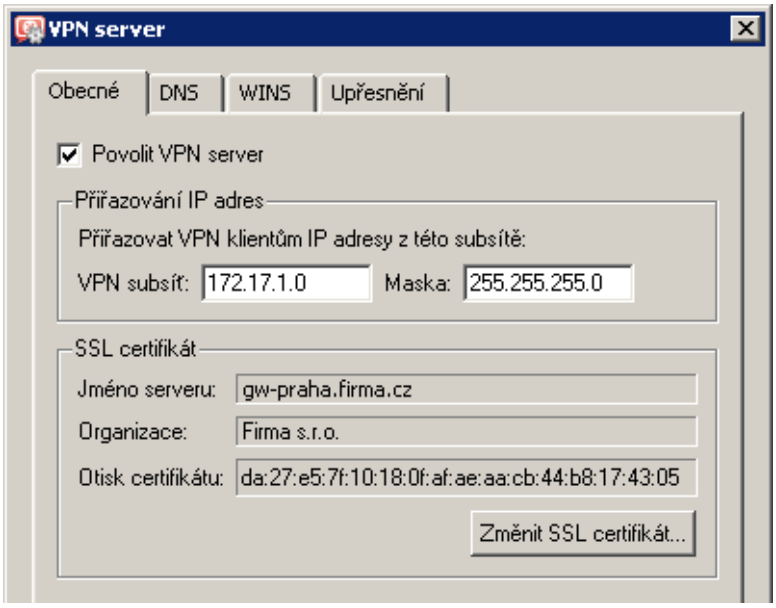
Obrázek 23.18 Centrála — konfigurace TCP/IP na rozhraní firewallu připojeném do lokální sítě

- Na ostatních počítačích rovněž nastavíme jako upřednostňovaný (primární) DNS server IP adresu `10.1.1.1`.

Poznámka: Pro správnou funkci DNS musí DNS databáze obsahovat záznamy o počítačích v příslušné lokální síti. Toho lze docílit zapsáním IP adres a DNS jmen lokálních počítačů do souboru `hosts` (v případě statických IP adres) nebo nastavením spolupráce modulu *DNS* s DHCP serverem (v případě dynamicky přidělovaných IP adres). Podrobnosti viz kapitola 8.1.

4. Povolíme VPN server, případně nastavíme jeho SSL certifikát (nemáme-li certifikát vystavený důvěryhodnou certifikační autoritou, vytvoříme certifikát podepsaný sám sebou).

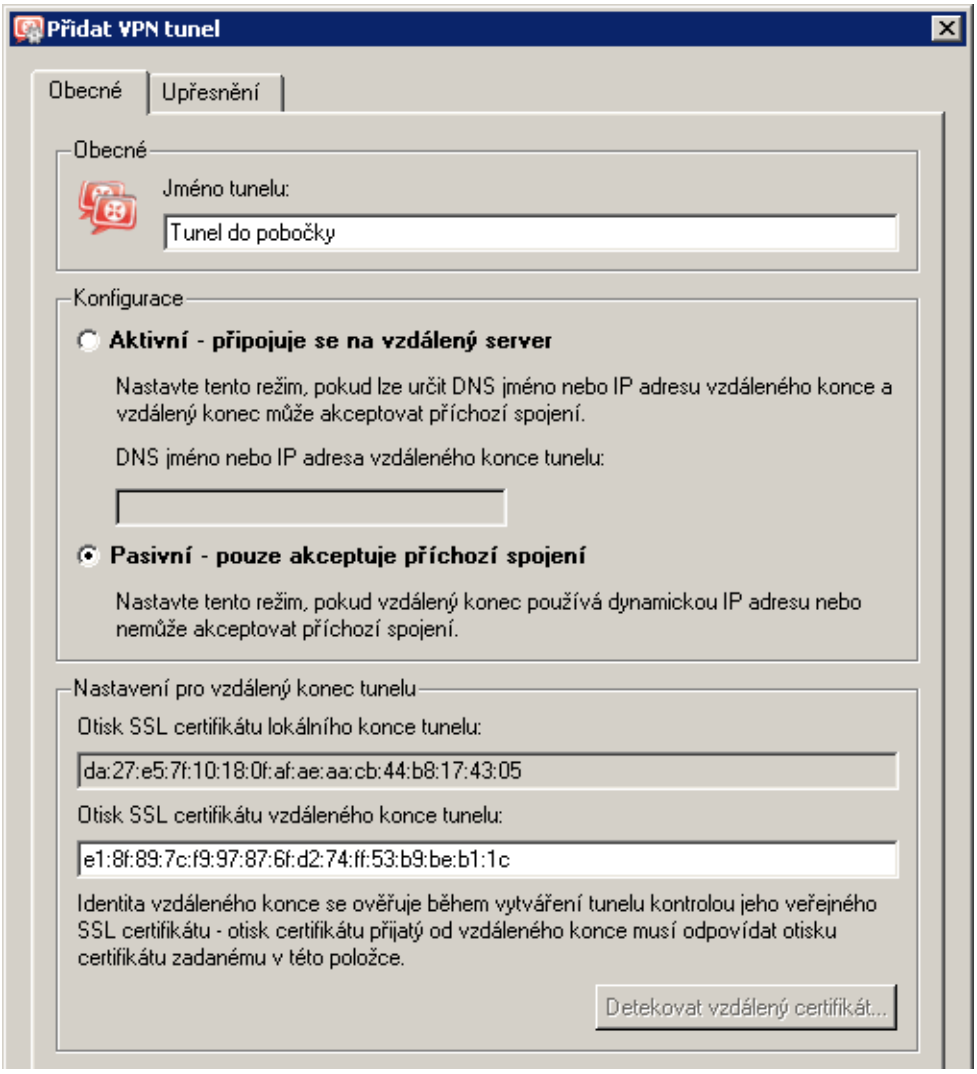
   Poznámka: V položkách *VPN subsít'* a *Maska* je nyní uvedena automaticky vybraná volná subsíť.



Obrázek 23.19 Centrála — konfigurace VPN serveru

Podrobnosti o konfiguraci VPN serveru viz kapitola 23.1.

5. Vytvoříme pasivní konec VPN tunelu (server pobočky má dynamickou IP adresu). Jako otisk vzdáleného SSL certifikátu zadáme otisk certifikátu VPN serveru na pobočce.



Obrázek 23.20 Centrála — definice VPN tunelu do pobočky

6. Upravíme komunikační pravidla dle požadavků na omezení přístupu.
   - V pravidle *Lokální komunikace* ponecháme pouze lokální síť centrály firmy, tj. firewall a sítě `LAN 1` a `LAN 2`.
   - Přidáme pravidlo *VPN klienti* povolující přístup VPN klientů do sítě `LAN 1` a do sítě pobočky firmy (přes VPN tunel).
   - Přidáme pravidlo *Pobočka* povolující přístup do sítě `LAN 1` v centrále k požadovaným službám.
   - Přidáme pravidlo *Centrála* povolující přístup z obou subsítí v centrále do sítě pobočky.

   Takto definovaná pravidla splňují všechny požadavky na povolení a omezení přístupu mezi centrálou, pobočkou a VPN klienty. Komunikace, která nevyhoví těmto pravidlům,

Jméno	Zdroj	Cíl	Služba	Akce
Služba Kerio VPN	Internet	Firewall	Kerio VPN	✓
Lokální komunikace	Firewall Důvěryhodné / lokální	Firewall Důvěryhodné / lokální	Libovolný	✓
VPN klienti	Všichni VPN klienti	LAN 1 Tunel do pobočky	Libovolný	✓
Pobočka	Tunel do pobočky	LAN 1	Libovolný	✓
Centrála	Důvěryhodné / lokální	Tunel do pobočky	Libovolný	✓
Komunikace firewallu	Firewall	Libovolný	Libovolný	✓

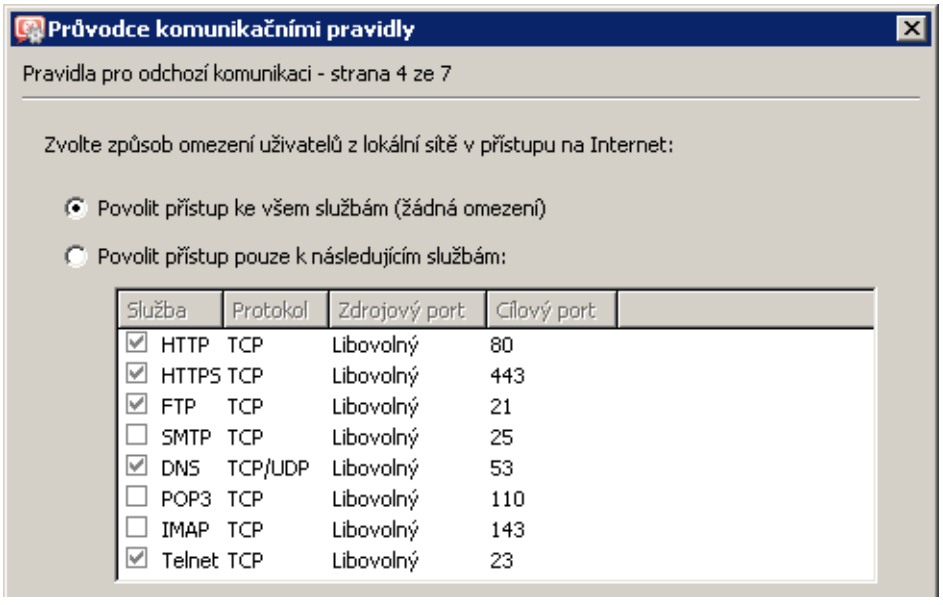
Obrázek 23.21 Centrála — výsledná komunikační pravidla

bude implicitně blokována výchozím pravidlem (viz kapitola 7.3).

Konfigurace v pobočce firmy

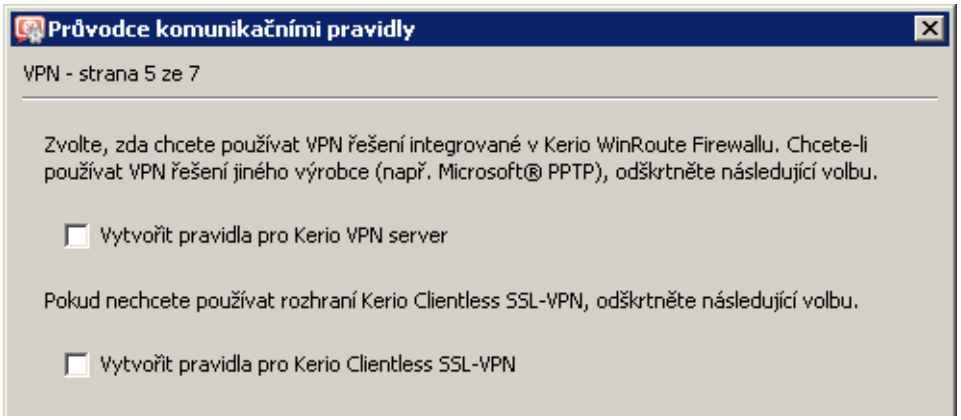
1. Na výchozí bránu sítě pobočky (dále jen „server“) nainstalujeme *WinRoute* (verze `6.0.0` nebo vyšší).

2. Ve *WinRoute* nastavíme základní komunikační pravidla pomocí *Průvodce komunikačními pravidly* (viz kapitola 7.1). Pro jednoduchost předpokládejme, že nebudeme omezovat přístup z lokální sítě do Internetu, tzn. ve 4. kroku průvodce povolíme přístup ke všem službám.



Obrázek 23.22 Pobočka — přístup z lokální sítě do Internetu bez omezení

Vytvářet pravidla pro *Kerio VPN server* a *Kerio Clientless SSL-VPN* v tomto případě nemá smysl (server má dynamickou veřejnou IP adresu). V 5. kroku průvodce proto ponecháme obě volby vypnuté.



Obrázek 23.23 Pobočka — pravidla pro Kerio VPN server není třeba vytvářet

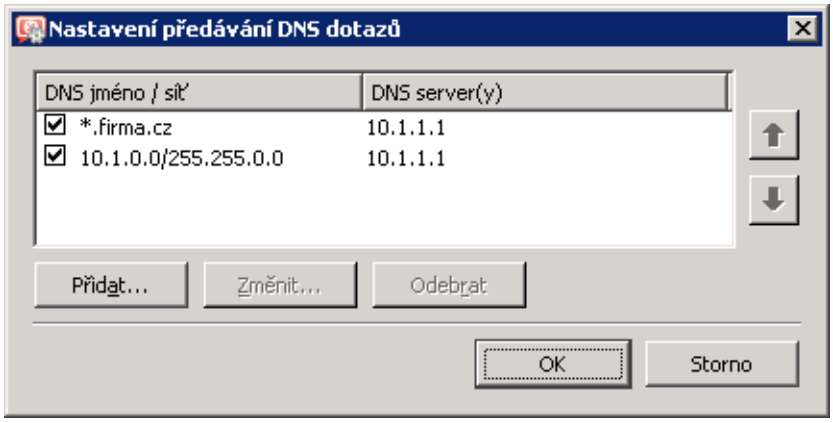
Tím dojde k vytvoření pravidel pro připojení k VPN serveru a pro komunikaci VPN klientů s lokální sítí, resp. firewallem.

Jméno	Zdroj	Cíl	Služba	Akce
Služba Kerio VPN	Internet	Firewall	Kerio VPN	✓
Lokální komunikace	Firewall Všichni VPN klienti Důvěryhodné / lokální	Firewall Všichni VPN klienti Důvěryhodné / lokální	Libovolný	✓
Komunikace firewallu	Firewall	Libovolný	Libovolný	✓

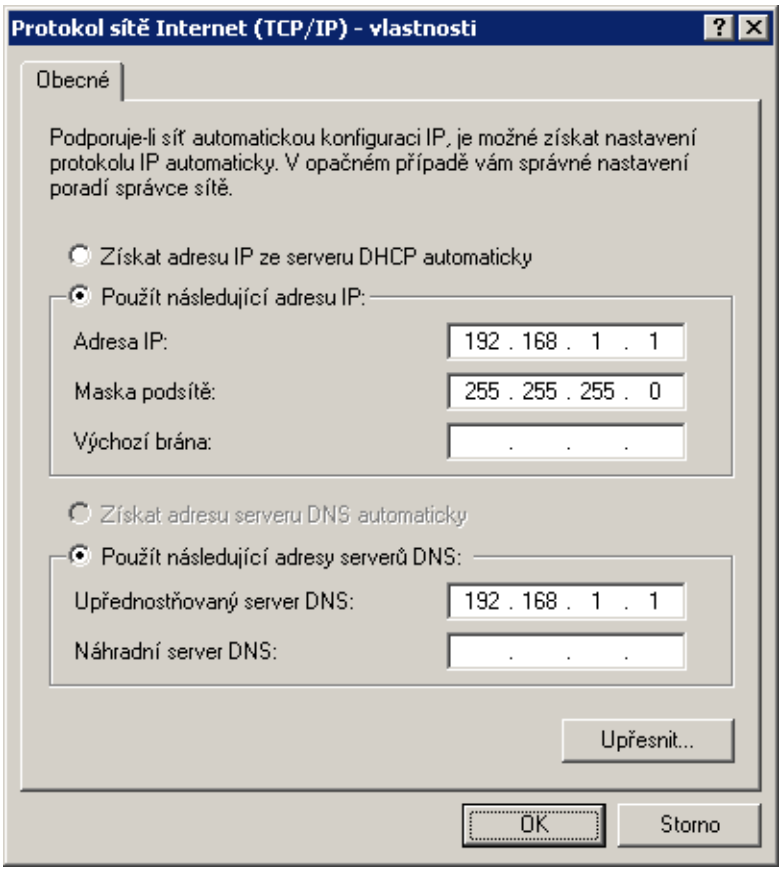
Obrázek 23.24 Pobočka — výchozí komunikační pravidla pro Kerio VPN

Po vytvoření VPN tunelu tato pravidla upravíme (viz 6. krok).

3. Nastavíme DNS (resp. upravíme nastavení DNS):
   - V konfiguraci modulu *DNS* ve *WinRoute* povolíme službu *DNS forwarder* (předávání DNS dotazů jiným serverům).
   - Zapneme volbu *Použít nastavení pro předávání DNS dotazů* a definujeme pravidla pro jména v doméně `firma.cz`. Jako DNS server pro předávání dotazů uvedeme IP adresu vnitřního rozhraní počítače s *WinRoute* na protější straně tunelu (tj. rozhraní připojeného do lokální sítě na protější straně).
   - Na rozhraní počítače s *WinRoute* připojeném do lokální sítě nastavíme jako upřednostňovaný (primární) DNS server IP adresu tohoto rozhraní (tj. `192.168.1.1`).



Obrázek 23.25 Pobočka — nastavení předávání DNS dotazů



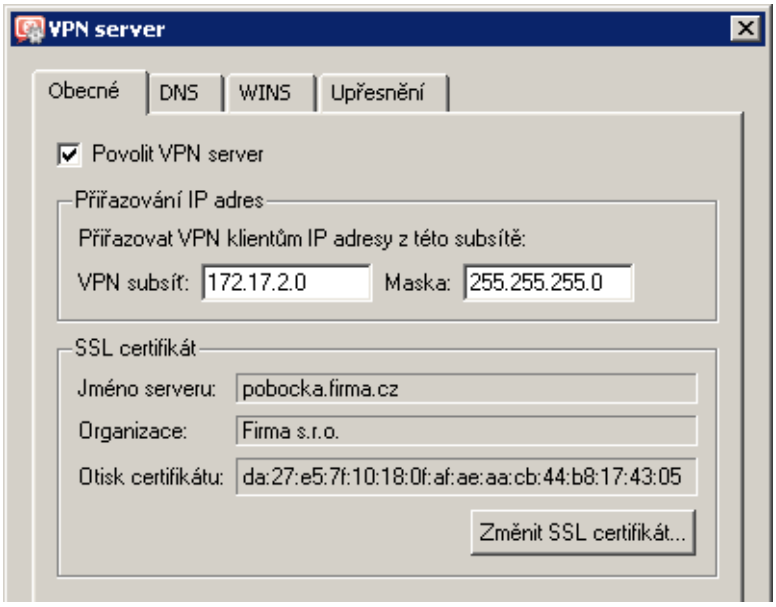
Obrázek 23.26 Pobočka — konfigurace TCP/IP na rozhraní firewallu připojeném do lokální sítě

- Na ostatních počítačích rovněž nastavíme jako upřednostňovaný (primární) DNS server IP adresu `192.168.1.1`.

Poznámka: Pro správnou funkci DNS musí DNS databáze obsahovat záznamy o počítačích v příslušné lokální síti. Toho lze docílit zapsáním IP adres a DNS jmen lokálních počítačů do souboru `hosts` (v případě statických IP adres) nebo nastavením spolupráce modulu *DNS* s DHCP serverem (v případě dynamicky přidělovaných IP adres). Podrobnosti viz kapitola 8.1.

4. Povolíme VPN server, případně nastavíme jeho SSL certifikát (nemáme-li certifikát vystavený důvěryhodnou certifikační autoritou, vytvoříme certifikát podepsaný sám sebou).

   Poznámka: V položkách *VPN subsíť* a *Maska* je nyní uvedena automaticky vybraná volná subsíť.



Obrázek 23.27 Pobočka — konfigurace VPN serveru

   Podrobnosti o konfiguraci VPN serveru viz kapitola 23.1.

5. Vytvoříme aktivní konec VPN tunelu připojující se k serveru centrály (`praha.firma.cz`). Jako otisk vzdáleného SSL certifikátu zadáme otisk certifikátu VPN serveru v centrále.

   V tomto okamžiku by mělo dojít ke spojení — navázání tunelu. Je-li spojení úspěšné, zobrazí se u obou konců tunelu ve sloupci *Informace o adaptéru* stav *Připojeno*. Nedojde-li k navázání spojení, doporučujeme prověřit nastavení komunikačních pravidel a dostupnost vzdáleného serveru — v našem příkladu můžeme na serveru pobočky zadat příkaz

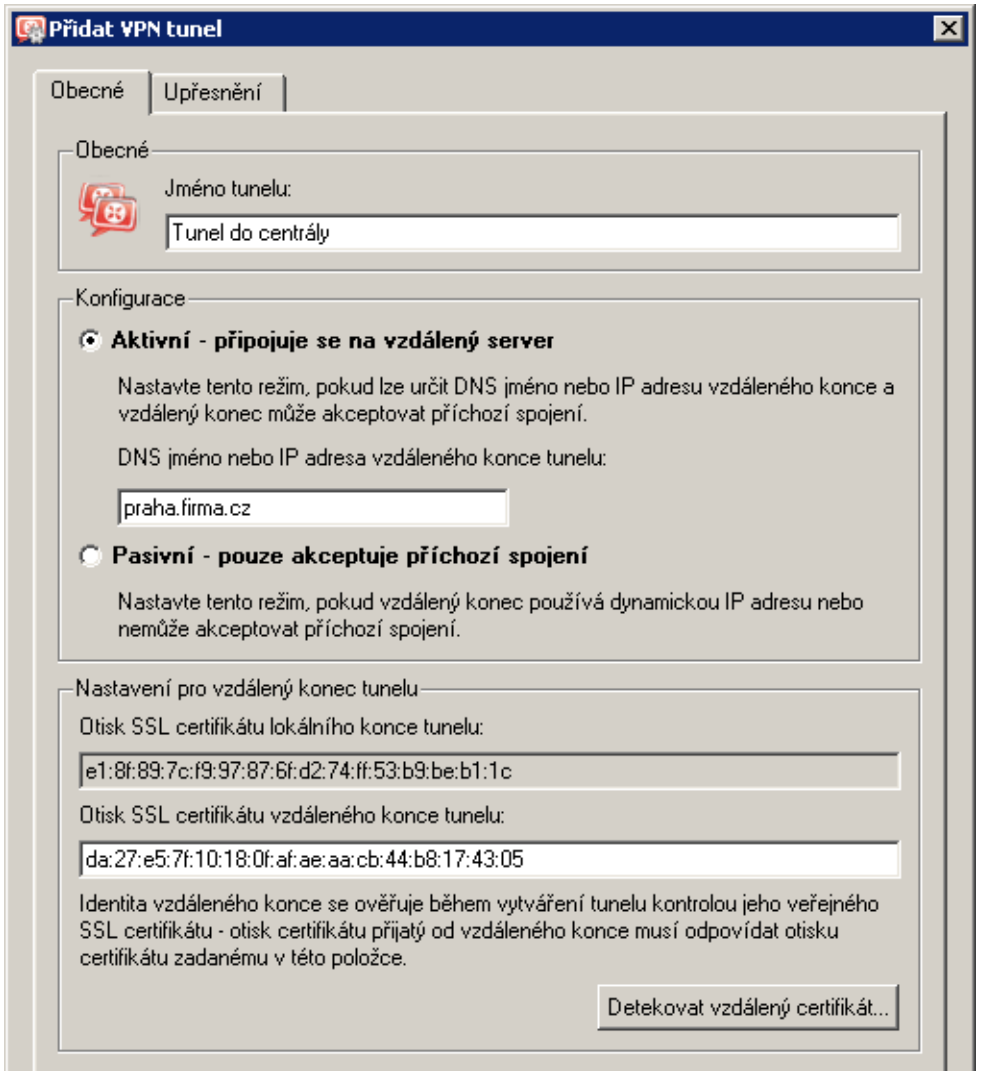
   ```
   ping praha.firma.cz
   ```

   Poznámka: Je-li po navázání tunelu detekována kolize VPN subsítě se vzdálenou sítí, vybereme vhodnou volnou subsíť a nastavíme ji ve VPN serveru (viz 4. krok).

   Podrobnosti o vytváření VPN tunelů viz kapitola 23.3.

6. Do komunikačního pravidla *Lokální komunikace* přidáme vytvořený VPN tunel. Zároveň můžeme z tohoto pravidla odstranit nevyužité rozhraní *Dial-In* a skupinu *VPN klienti* (do pobočky se žádní VPN klienti připojovat nemohou).

   Poznámka: Žádné další úpravy komunikačních pravidel není třeba provádět. Požadovaná omezení přístupu jsou již zajištěna komunikačními pravidly na serveru centrály.



Obrázek 23.28 Pobočka — definice VPN tunelu do centrály

Jméno	Zdroj	Cíl	Služba	Akce
Služba Kerio VPN	Internet	Firewall	Kerio VPN	✓
Lokální komunikace	Firewall Všichni VPN klienti Tunel do centrály Důvěryhodné / lokální	Firewall Všichni VPN klienti Tunel do centrály Důvěryhodné / lokální	Libovolný	✓
Komunikace firewallu	Firewall	Libovolný	Libovolný	✓

Obrázek 23.29 Pobočka — výsledná komunikační pravidla

Test funkčnosti VPN

Konfigurace VPN tunelu je dokončena. Nyní doporučujeme z každé lokální sítě vyzkoušet dostupnost počítačů v síti na protější straně tunelu.

Jako testovací nástroj lze použít např. příkazy operačního systému `ping` nebo `tracert`. Doporučujeme ověřit dostupnost počítače ve vzdálené síti zadaného jednak IP adresou, jednak DNS jménem.

Nedostaneme-li odezvu při zadání vzdáleného počítače IP adresou, je třeba hledat chybu v nastavení komunikačních pravidel, případně prověřit, zda nenastala kolize subsítí (stejná subsíť na obou stranách tunelu).

Je-li test při zadání počítače IP adresou úspěšný, ale při zadání počítače DNS jménem je hlášena chyba (*Neznámý hostitel*), pak je třeba prověřit konfiguraci DNS.

23.6 Složitější konfigurace Kerio VPN: firma s více pobočkami

V této kapitole uvádíme příklad složitější konfigurace VPN, kdy mezi propojenými privátními sítěmi vznikají redundantní cesty (tzn. mezi dvěma sítěmi existuje více různých cest, kterými mohou být pakety směrovány).

Oproti VPN bez redundantních cest (viz kapitola 23.5) se konfigurace *Kerio VPN* liší pouze v nastavení směrování mezi konci jednotlivých tunelů. V tomto případě je třeba nastavit směrování mezi jednotlivými konci VPN tunelů ručně, použití automatické výměny cest není vhodné. Důvodem je, že *Kerio VPN* nepoužívá žádný směrovací protokol a výměna cest probíhá pouze na základě porovnání směrovacích tabulek na jednotlivých koncích VPN tunelu (viz též kapitola 23.4). Při použití automatické výměny cest nebude směrování mezi jednotlivými sítěmi optimální!

Konfigurace je z důvodu názornosti popsána na příkladu firmy s centrálou a dvěma pobočkami, jejichž lokální privátní sítě jsou vzájemně propojené VPN tunely (tzv. trojúhelníkové schéma). Tento příklad lze zobecnit pro libovolný počet vzájemně propojených privátních sítí.

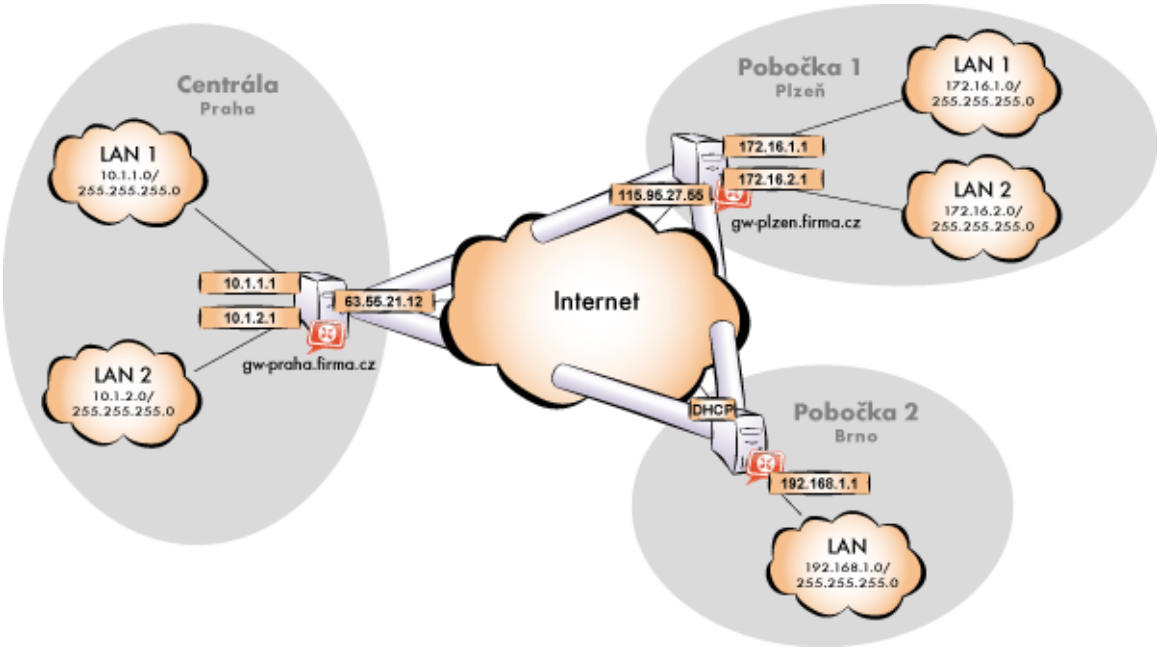
Uvedený příklad je zaměřen na konfiguraci VPN tunelů a správné nastavení směrování mezi jednotlivými privátními sítěmi; nezabývá se omezováním přístupu. Možnosti omezení přístupu v rámci VPN ukazuje příklad v kapitole 23.5.

Zadání

Předpokládejme schéma sítě dle obrázku 23.30.

Server (výchozí brána) centrály má pevnou veřejnou IP adresu `63.55.21.12` (DNS jméno `gw-praha.firma.cz`). Server první pobočky má IP adresu `115.95.27.55` (DNS jméno `gw-plzen.firma.cz`), server druhé pobočky má dynamickou IP adresu přidělovanou poskytovatelem internetového připojení.

Centrála používá DNS doménu `firma.cz`, pobočky používají subdomény `plzen.firma.cz` a `brno.firma.cz`. Konfigurace jednotlivých lokálních sítí a použité IP adresy jsou uvedeny ve schématu.



Obrázek 23.30 Příklad konfigurace VPN — firma se dvěma pobočkami

Obecný postup

Ve všech lokálních sítích (tj. v centrále i v obou pobočkách firmy) je třeba provést tyto kroky:

1. Na výchozí bráně sítě musí být nainstalován *WinRoute* verze `6.1.0` nebo vyšší. Starší verze neumožňují nastavení směrování (vlastních cest) pro VPN tunely, a nelze je proto použít pro uvažovanou konfiguraci VPN (viz obrázek 23.30).

   Poznámka: Pro *každou* instalaci *WinRoute* je potřeba samostatná licence pro příslušný počet uživatelů! Podrobnosti viz kapitola 4.

2. Nastavíme a otestujeme přístup z lokální sítě do Internetu. Počítače v lokální síti musí mít jako výchozí bránu a upřednostňovaný (primární) DNS server nastavenu IP adresu počítače s *WinRoute*.

   Jedná-li se o novou (čistou) instalaci *WinRoute*, můžeme využít průvodce komunikačními pravidly (viz kapitola 7.1).

   Podrobný popis základní konfigurace *WinRoute* a lokální sítě je uveden v samostatném manuálu *Kerio WinRoute Firewall — konfigurace krok za krokem*.

3. V konfiguraci modulu *DNS* nastavíme pravidla pro předávání DNS dotazů pro domény ostatních poboček. Tím umožníme přístup na počítače ve vzdálených sítích jejich DNS jmény (v opačném případě by bylo nutné zadávat vzdálené počítače IP adresami).

   Pro správné předávání DNS dotazů z počítače s *WinRoute* musíme na tomto počítači nastavit primární DNS server „sám na sebe“ (tzn. použít IP adresu některého síťového rozhraní tohoto počítače). Jako sekundární DNS server pak musí být specifikován server, na který

budou předávány DNS dotazy do ostatních domén (typicky DNS server poskytovatele internetového připojení).

Poznámka: Pro správnou funkci DNS musí DNS databáze obsahovat záznamy o počítačích v příslušné lokální síti. Toho lze docílit zapsáním IP adres a DNS jmen lokálních počítačů do souboru `hosts` (v případě statických IP adres) nebo nastavením spolupráce *DNS* s DHCP serverem (v případě dynamicky přidělovaných IP adres). Podrobnosti viz kapitola 8.1.

4. V sekci *Rozhraní* povolíme VPN server, případně nastavíme jeho SSL certifikát. Poznamenáme si otisk certifikátu serveru — budeme jej potřebovat při konfiguraci VPN tunelů ve zbývajících pobočkách.

   Zkontrolujeme, zda automaticky vybraná VPN subsíť nekoliduje s žádnou lokální subsítí v žádné pobočce; případně vybereme jinou volnou subsíť.

   Poznámka: Vzhledem ke složitosti uvažované VPN doporučujeme předem vyhradit tři volné subsítě, které přidělíme jednotlivým VPN serverům.

5. Definujeme VPN tunel do jedné ze vzdálených sítí. Pasivní konec tunelu musí být vytvořen na serveru, který má pevnou veřejnou IP adresu. Na serveru s dynamickou IP adresou lze vytvářet pouze aktivní konce VPN tunelů.

   Nastavíme směrování (vlastní cesty) pro tento tunel. Zvolíme *Používat pouze vlastní cesty* a do seznamu vlastních cest uvedeme všechny subsítě ve vzdálené síti.

   Je-li protější konec tunelu již definován, zkontrolujeme, zda došlo ke spojení (navázání) tunelu. V případě neúspěchu prohlédneme záznam *Error*, zkontrolujeme otisky certifikátů a prověříme dostupnost vzdáleného serveru.

6. Obdobným způsobem definujeme tunel a nastavíme směrování do druhé vzdálené sítě.

7. Povolíme komunikaci mezi lokální sítí a vzdálenými sítěmi. Chceme-li povolit komunikaci bez omezení, stačí vytvořené VPN tunely přidat do položek *Zdroj* a *Cíl* v komunikačním pravidle *Lokální komunikace*. Možnosti omezování přístupu v rámci VPN ukazuje příklad v kapitole 23.5.

8. Z každé lokální sítě otestujeme dostupnost počítačů v obou vzdálených sítích. Pro tento test můžeme použít systémové příkazy `ping` a `tracert`. Ověříme dostupnost počítače ve vzdálené síti zadaného jednak IP adresou, jednak DNS jménem.

   Nedostaneme-li odezvu při zadání vzdáleného počítače IP adresou, je třeba hledat chybu v nastavení komunikačních pravidel, případně prověřit, zda nenastala kolize subsítí (stejná subsíť na obou stranách tunelu).

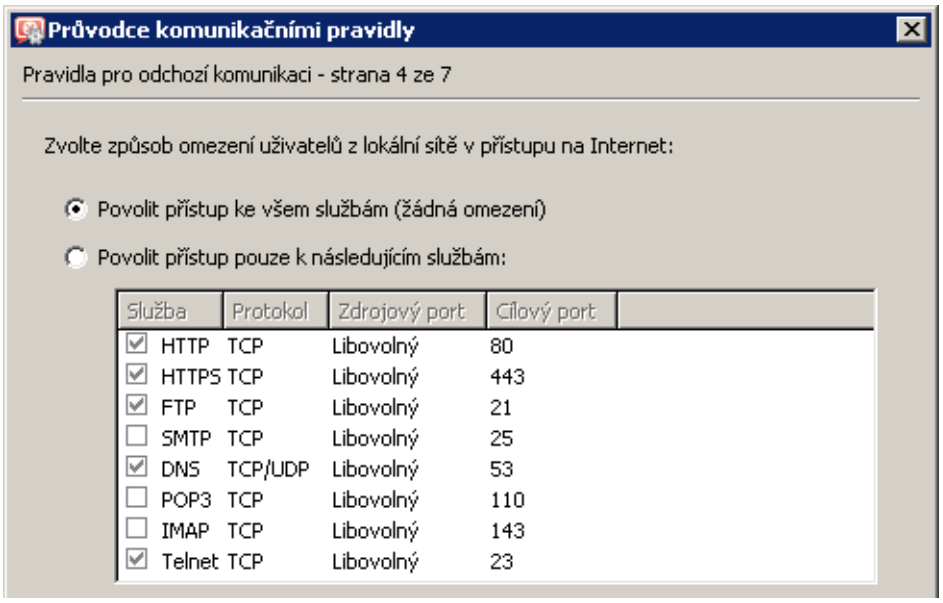
   Je-li test při zadání počítače IP adresou úspěšný, ale při zadání počítače DNS jménem je hlášena chyba (*Neznámý hostitel*), pak je třeba prověřit konfiguraci DNS.

Následující sekce podrobně popisují konfiguraci *Kerio VPN* v centrále a v pobočkách firmy.

Konfigurace v centrále firmy

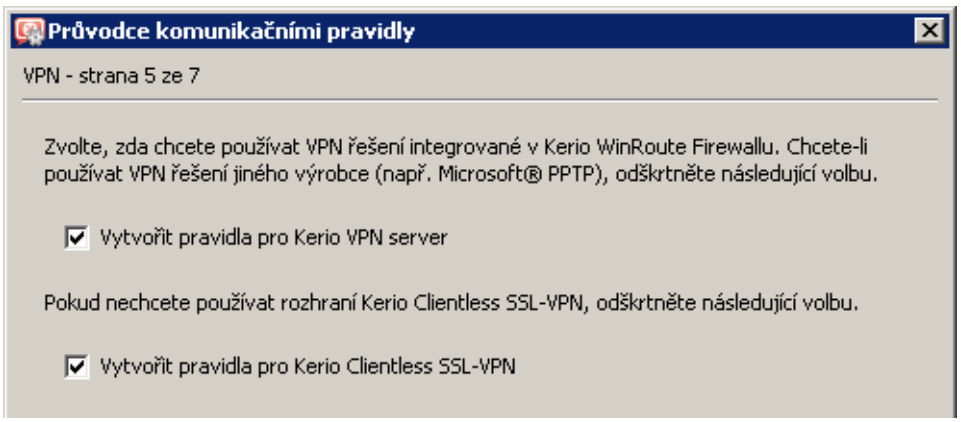
1. Na výchozí bránu sítě centrály nainstalujeme *WinRoute* (verze `6.1.0` nebo vyšší).

2. Ve *WinRoute* nastavíme základní komunikační pravidla pomocí *Průvodce komunikačními pravidly* (viz kapitola 7.1). Pro jednoduchost předpokládejme, že nebudeme omezovat přístup z lokální sítě do Internetu, tzn. ve 4. kroku průvodce povolíme přístup ke všem službám.



Obrázek 23.31 Centrála — přístup z lokální sítě do Internetu bez omezení

V 5. kroku průvodce zvolíme *Vytvořit pravidla pro Kerio VPN server*. Na nastavení volby *Vytvořit pravidla pro Kerio Clientless SSL-VPN* nezáleží (tento příklad se nezabývá rozhraním *Clientless SSL-VPN*).



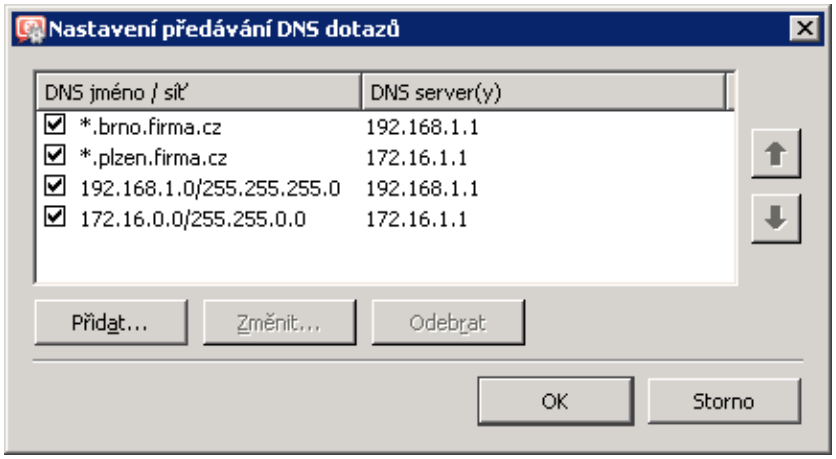
Obrázek 23.32 Centrála — vytvoření výchozích komunikačních pravidel pro Kerio VPN

Tím dojde k vytvoření pravidel pro připojení k VPN serveru a pro komunikaci VPN klientů s lokální sítí, resp. firewallem.

Jméno	Zdroj	Cíl	Služba	Akce
Služba Kerio VPN	Internet	Firewall	Kerio VPN	✓
Lokální komunikace	Firewall Všichni VPN klienti Důvěryhodné / lokální	Firewall Všichni VPN klienti Důvěryhodné / lokální	Libovolný	✓
Komunikace firewallu	Firewall	Libovolný	Libovolný	✓

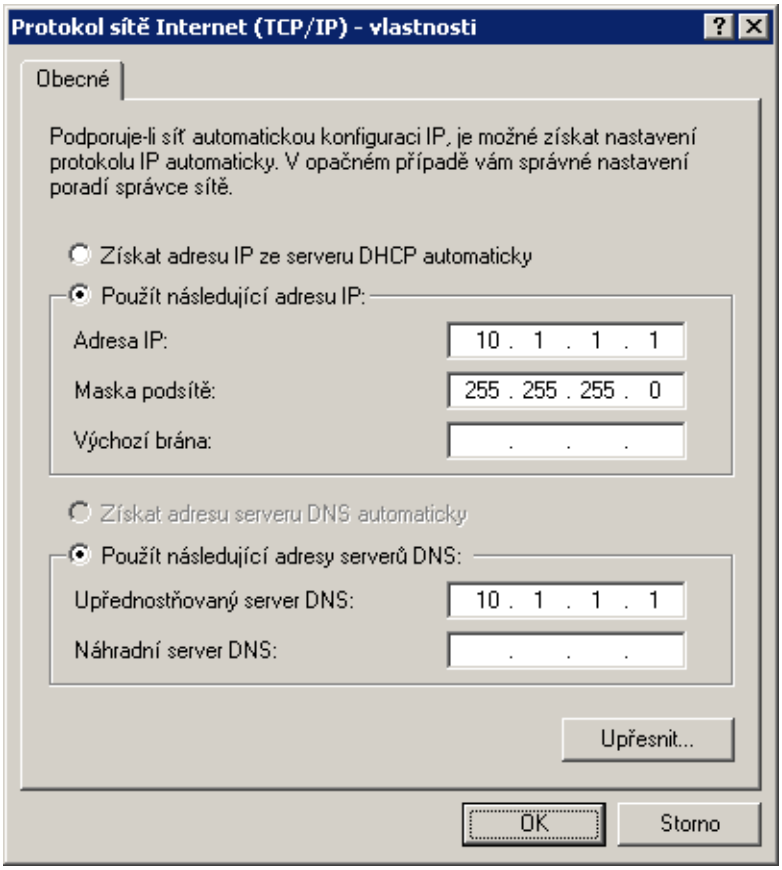
Obrázek 23.33 Centrála — výchozí komunikační pravidla pro Kerio VPN

3. Nastavíme DNS (resp. upravíme nastavení DNS):
   - V konfiguraci modulu *DNS* ve *WinRoute* povolíme službu *DNS forwarder* (předávání DNS dotazů jiným serverům).
   - Zapneme volbu *Použít nastavení pro předávání DNS dotazů* a definujeme pravidla pro jména v doménách `plzen.firma.cz` a `brno.firma.cz`. Jako DNS server pro předávání dotazů vždy uvedeme IP adresu vnitřního rozhraní počítače s *WinRoute* na protější straně příslušného tunelu (tj. rozhraní připojeného do lokální sítě na protější straně tunelu).



Obrázek 23.34 Centrála — nastavení předávání DNS dotazů

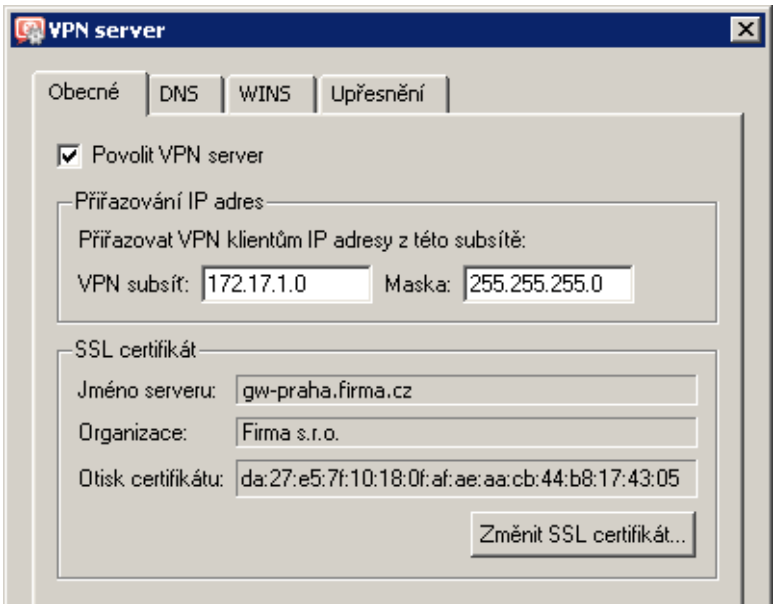
   - Na rozhraní počítače s *WinRoute* připojeném do lokální sítě *LAN 1* nastavíme jako upřednostňovaný (primární) DNS server IP adresu tohoto rozhraní (tj. `10.1.1.1`). Na rozhraní připojeném do lokální sítě *LAN 2* není třeba DNS nastavovat.
   - Na ostatních počítačích rovněž nastavíme jako upřednostňovaný (primární) DNS server IP adresu `10.1.1.1`.



Obrázek 23.35 Centrála — konfigurace TCP/IP na rozhraní firewallu připojeném do lokální sítě

4. Povolíme VPN server, případně nastavíme jeho SSL certifikát (nemáme-li certifikát vystavený důvěryhodnou certifikační autoritou, vytvoříme certifikát podepsaný sám sebou).

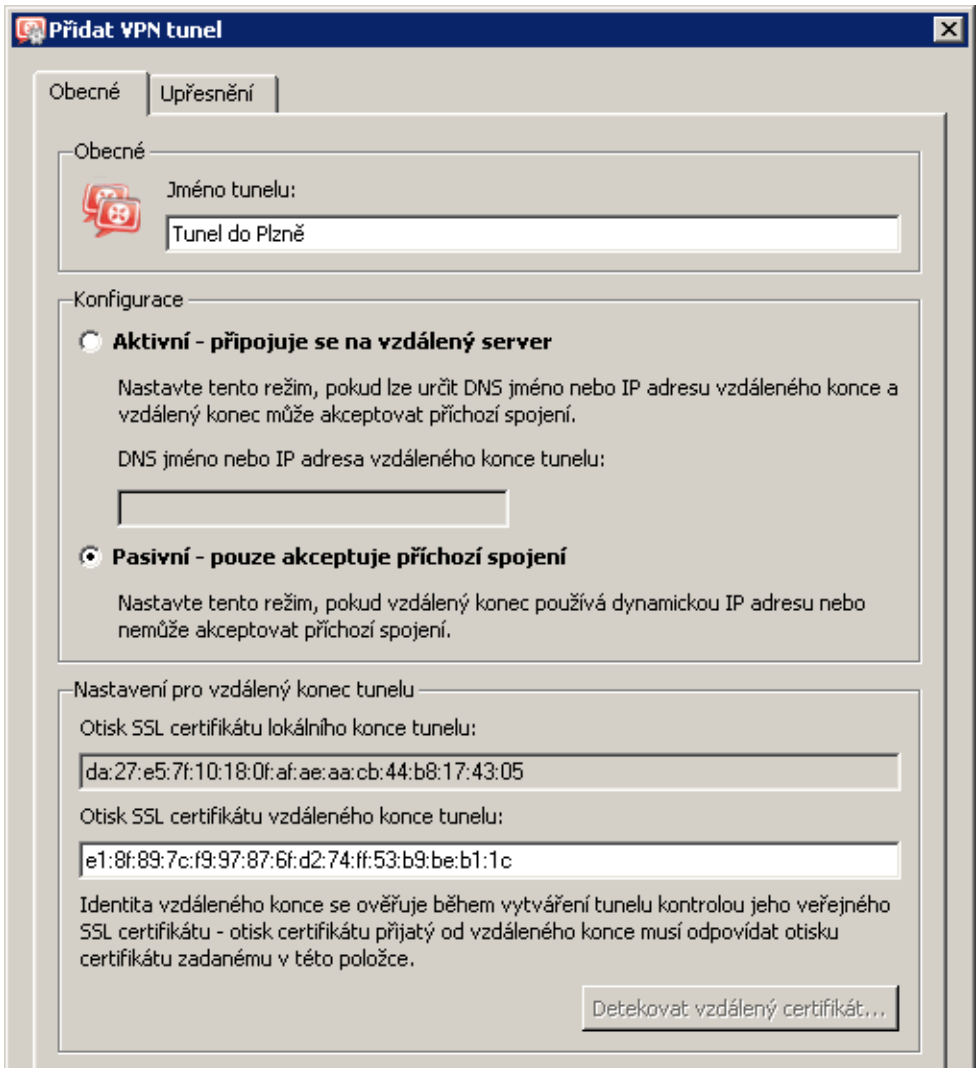
   Poznámka: V položkách *VPN subsíť* a *Maska* je nyní uvedena automaticky vybraná volná subsíť. Zkontrolujeme, zda tato subsíť nekoliduje s žádnou subsítí v centrále a na pobočkách, případně zadáme jinou (volnou) subsíť.



Obrázek 23.36 Centrála — konfigurace VPN serveru

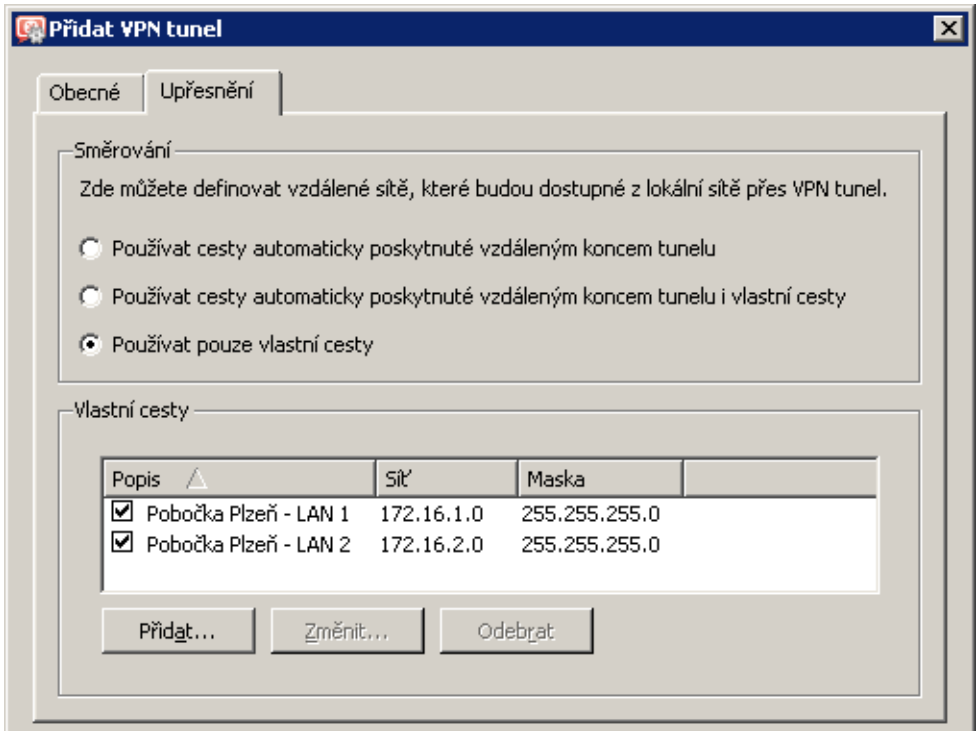
   Podrobnosti o konfiguraci VPN serveru viz kapitola 23.1.

5. Vytvoříme pasivní konec VPN tunelu do pobočky *Plzeň*. Jako otisk vzdáleného SSL certifikátu zadáme otisk certifikátu VPN serveru na v pobočce *Plzeň*.



Obrázek 23.37 Centrála — definice VPN tunelu do pobočky Plzeň

V záložce *Upřesnění* zvolíme *Používat pouze vlastní cesty* a nastavíme cesty do subsítí na vzdáleném konci tunelu (tj. v pobočce *Plzeň*).

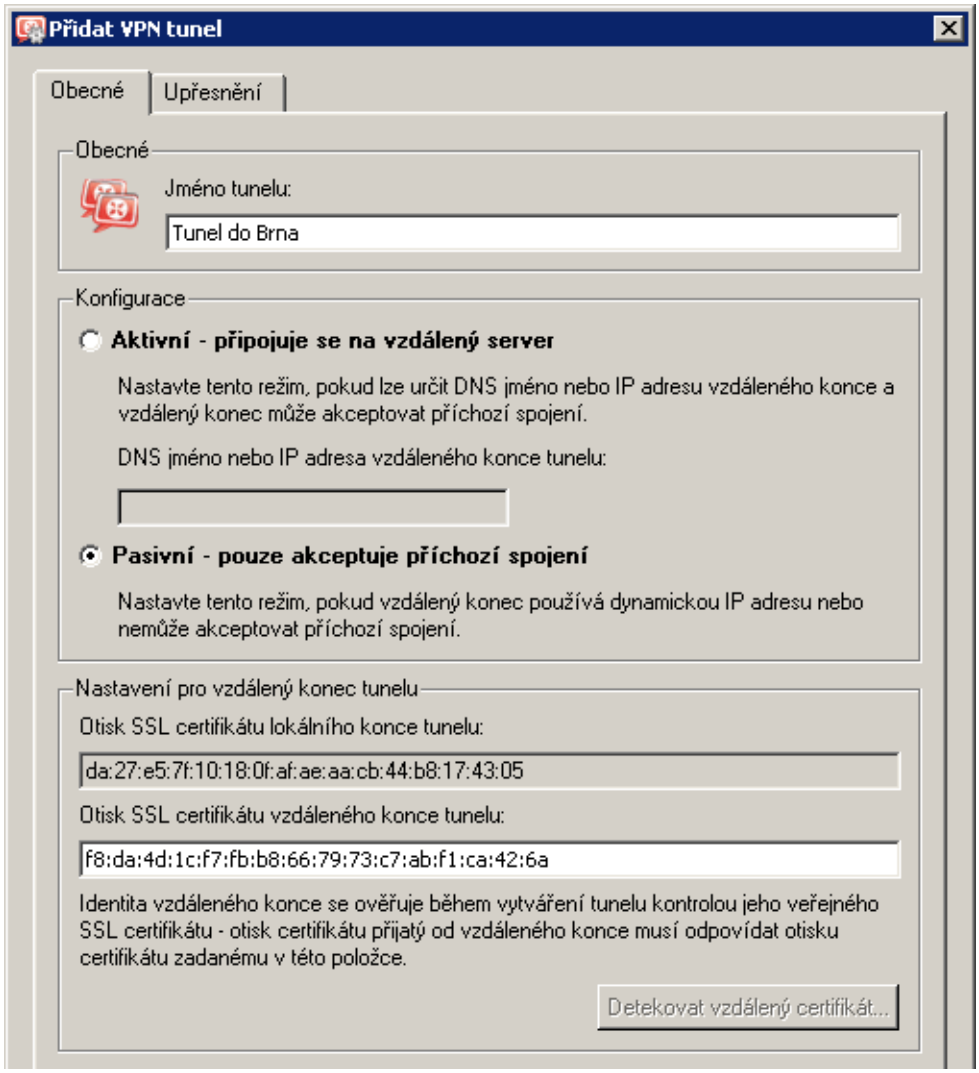


Obrázek 23.38 Centrála — nastavení směrování pro tunel do pobočky Plzeň

Upozornění

V případě konfigurace VPN podle uvažovaného schématu (viz obrázek 23.30) *nedoporučujeme* používat automaticky poskytnuté cesty! Při automatické výměně cest nebude směrování v rámci VPN optimální (např. veškerá komunikace mezi *centrálou* a pobočkou *Brno* bude směrována přes pobočku *Plzeň*, přičemž tunel mezi *centrálou* a pobočkou *Brno* zůstane nevyužitý).

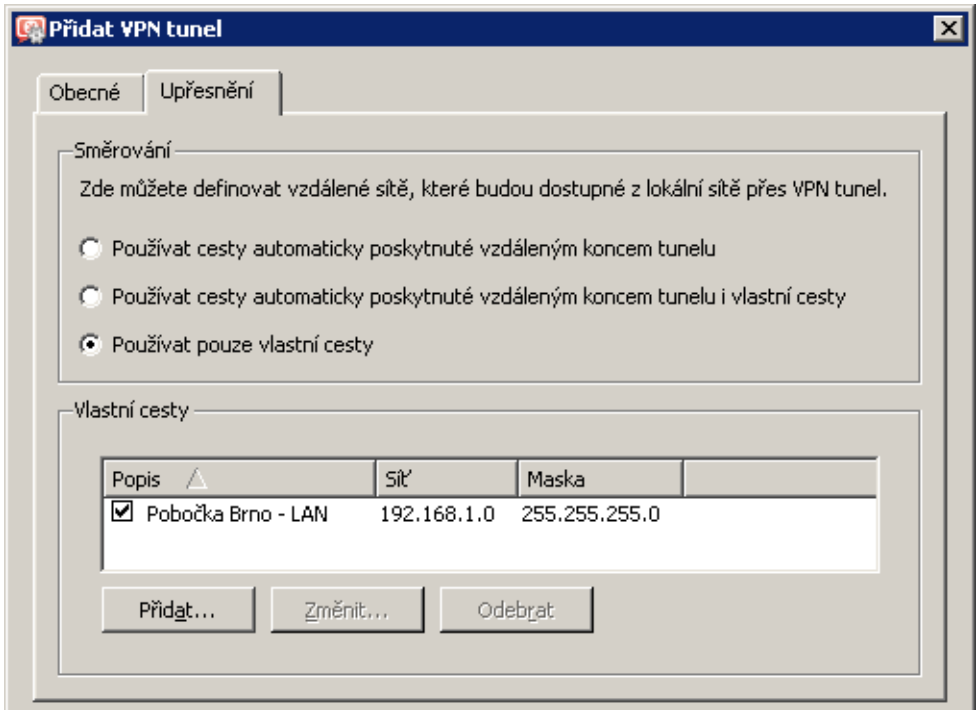
6. Obdobným způsobem vytvoříme pasivní konec tunelu do pobočky *Brno*.



Obrázek 23.39 Centrála — definice VPN tunelu do pobočky Brno

V záložce *Upřesnění* nastavíme volbu *Používat pouze vlastní cesty* a nastavíme cesty do subsítí na vzdáleném konci tunelu (tj. v pobočce *Brno*).

7. Do komunikačního pravidla *Lokální komunikace* přidáme vytvořené VPN tunely.



Obrázek 23.40 Centrála — nastavení směrování pro tunel do pobočky Brno

Jméno	Zdroj	Cíl	Služba	Akce
Služba Kerio VPN	Internet	Firewall	Kerio VPN	✓
Lokální komunikace	Firewall Všichni VPN klienti Tunel do Brna Tunel do Plzně Důvěryhodné / lokální	Firewall Všichni VPN klienti Tunel do Brna Tunel do Plzně Důvěryhodné / lokální	Libovolný	✓
Komunikace firewallu	Firewall	Libovolný	Libovolný	✓

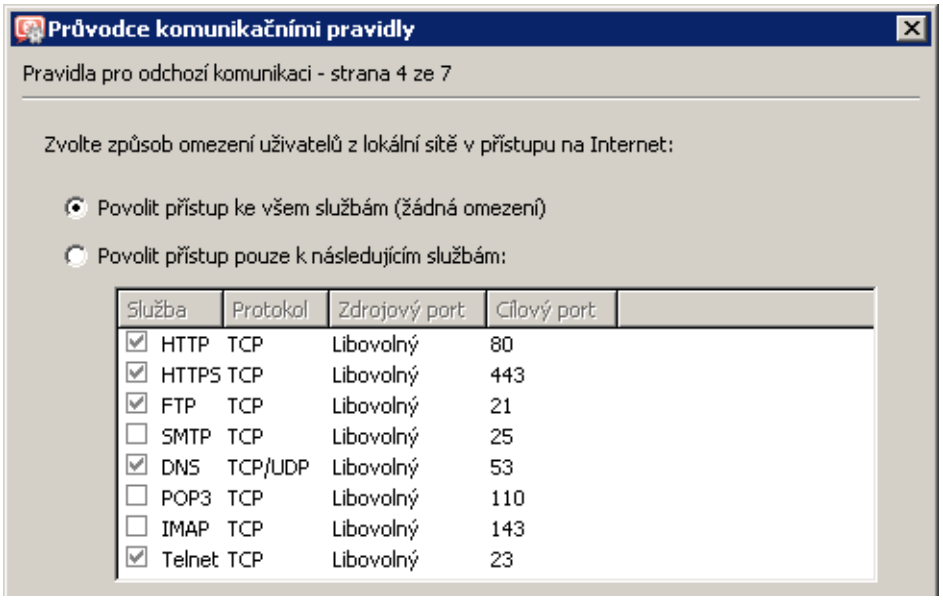
Obrázek 23.41 Centrála — výsledná komunikační pravidla

Konfigurace v pobočce Plzeň

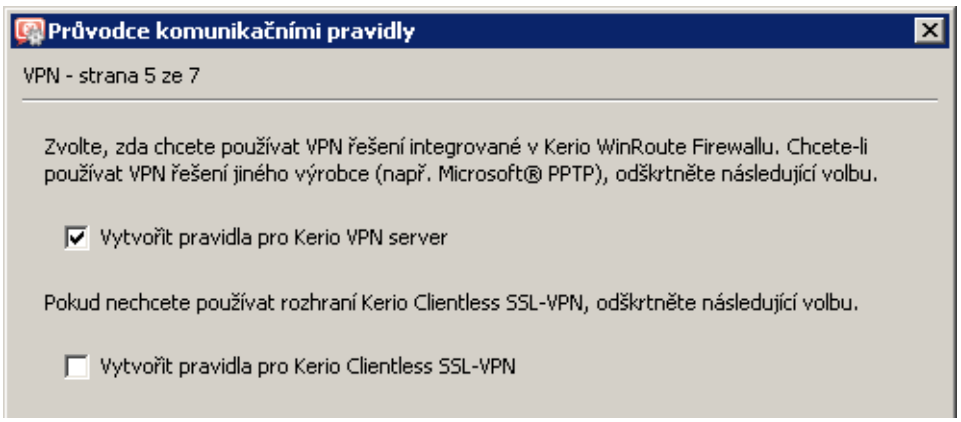
1. Na výchozí bránu sítě pobočky nainstalujeme *WinRoute* (verze `6.1.0` nebo vyšší).

2. Ve *WinRoute* nastavíme základní komunikační pravidla pomocí *Průvodce komunikačními pravidly* (viz kapitola 7.1). Pro jednoduchost předpokládejme, že nebudeme omezovat přístup z lokální sítě do Internetu, tzn. ve 4. kroku průvodce povolíme přístup ke všem službám.

   V 5. kroku průvodce zvolíme *Vytvořit pravidla pro Kerio VPN server* (na nastavení volby *Vytvořit pravidla pro Kerio Clientless SSL-VPN* nezáleží).



Obrázek 23.42 Pobočka Plzeň — přístup z lokální sítě do Internetu bez omezení



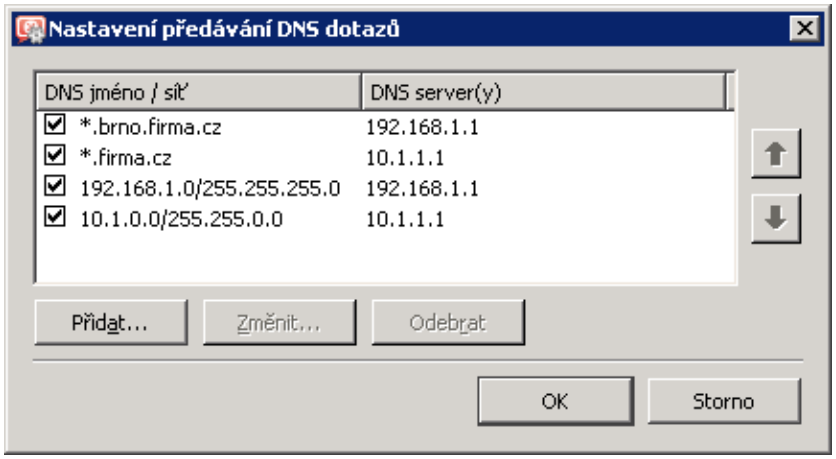
Obrázek 23.43 Pobočka Plzeň — vytvoření výchozích komunikačních pravidel pro Kerio VPN

Tím dojde k vytvoření pravidel pro připojení k VPN serveru a pro komunikaci VPN klientů s lokální sítí, resp. firewallem.

Jméno	Zdroj	Cíl	Služba	Akce
Služba Kerio VPN	Internet	Firewall	Kerio VPN	✓
Lokální komunikace	Firewall Všichni VPN klienti Důvěryhodné / lokální	Firewall Všichni VPN klienti Důvěryhodné / lokální	Libovolný	✓
Komunikace firewallu	Firewall	Libovolný	Libovolný	✓

Obrázek 23.44 Pobočka Plzeň — výchozí komunikační pravidla pro Kerio VPN

3. Nastavíme DNS (resp. upravíme nastavení DNS):
   - V konfiguraci modulu *DNS* ve *WinRoute* povolíme službu *DNS forwarder* (předávání DNS dotazů jiným serverům).
   - Zapneme volbu *Použít nastavení pro předávání DNS dotazů* a definujeme pravidla pro jména v doménách `firma.cz` a `brno.firma.cz`. Jako DNS server pro předávání dotazů vždy uvedeme IP adresu vnitřního rozhraní počítače s *WinRoute* na protější straně příslušného tunelu (tj. rozhraní připojeného do lokální sítě na protější straně).

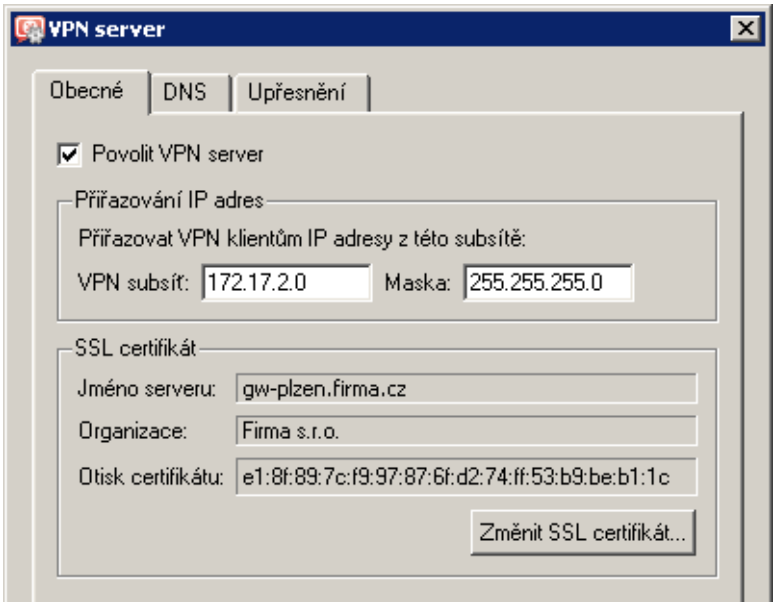


Obrázek 23.45 Pobočka Plzeň — nastavení předávání DNS dotazů

   - Na rozhraní počítače s *WinRoute* připojeném do lokální sítě *LAN 1* nastavíme jako upřednostňovaný (primární) DNS server IP adresu tohoto rozhraní (tj. `172.16.1.1`). Na rozhraní připojeném do lokální sítě *LAN 2* není třeba DNS nastavovat.
   - Na ostatních počítačích rovněž nastavíme jako upřednostňovaný (primární) DNS server IP adresu `172.16.1.1`.

4. Povolíme VPN server, případně nastavíme jeho SSL certifikát (nemáme-li certifikát vystavený důvěryhodnou certifikační autoritou, vytvoříme certifikát podepsaný sám sebou).

Poznámka: V položkách *VPN subsíť* a *Maska* je nyní uvedena automaticky vybraná volná subsíť. Zkontrolujeme, zda tato subsíť nekoliduje s žádnou subsítí v centrále a na pobočkách, případně zadáme jinou (volnou) subsíť.



Obrázek 23.46 Pobočka Plzeň — konfigurace VPN serveru

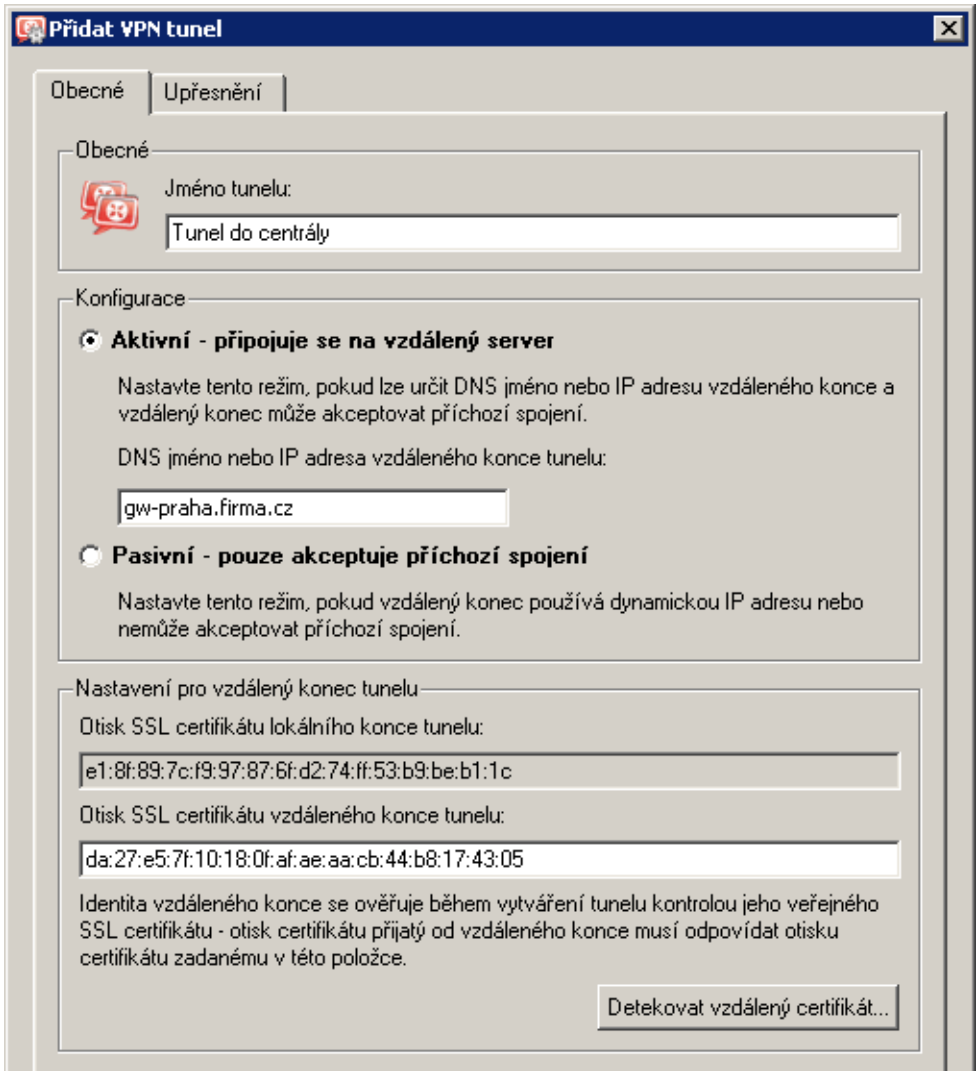
Podrobnosti o konfiguraci VPN serveru viz kapitola 23.1.

5. Vytvoříme aktivní konec VPN tunelu připojující se k serveru centrály (`praha.firma.cz`). Jako otisk vzdáleného SSL certifikátu zadáme otisk certifikátu VPN serveru v centrále.

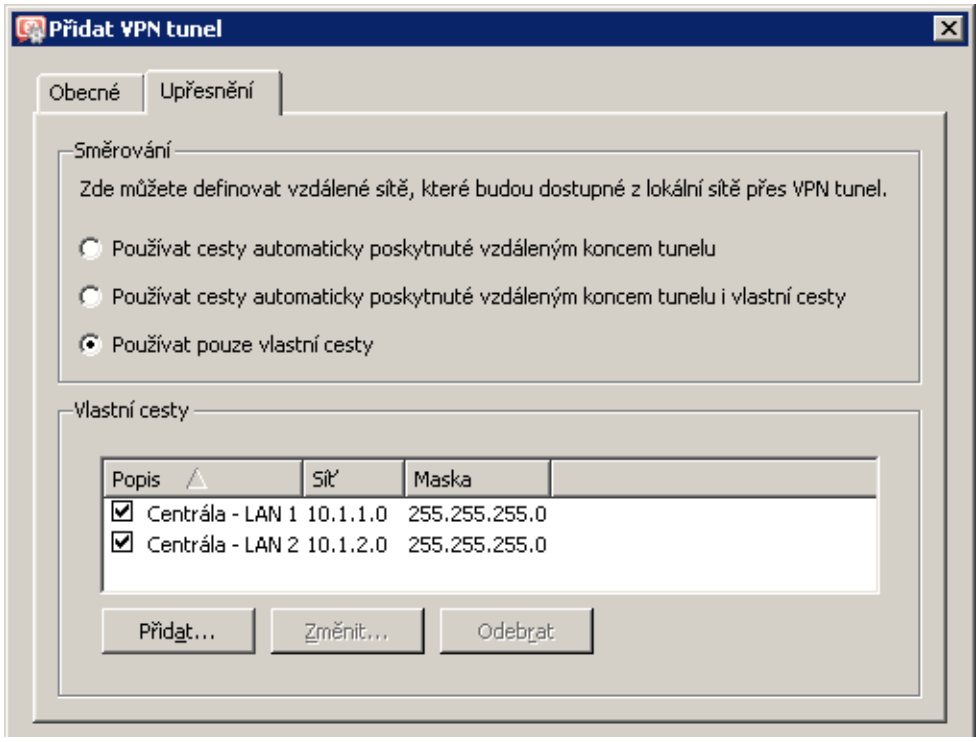
   V záložce *Upřesnění* zvolíme *Používat pouze vlastní cesty* a nastavíme cesty do lokálních sítí v *centrále*.

   V tomto okamžiku by mělo dojít ke spojení — navázání tunelu. Je-li spojení úspěšné, zobrazí se u obou konců tunelu ve sloupci *Informace o adaptéru* stav *Připojeno*. Nedojde-li k navázání spojení, doporučujeme prověřit nastavení komunikačních pravidel a dostupnost vzdáleného serveru — v našem příkladu můžeme na serveru pobočky *Plzeň* zadat příkaz

   ```
   ping gw-praha.firma.cz
   ```

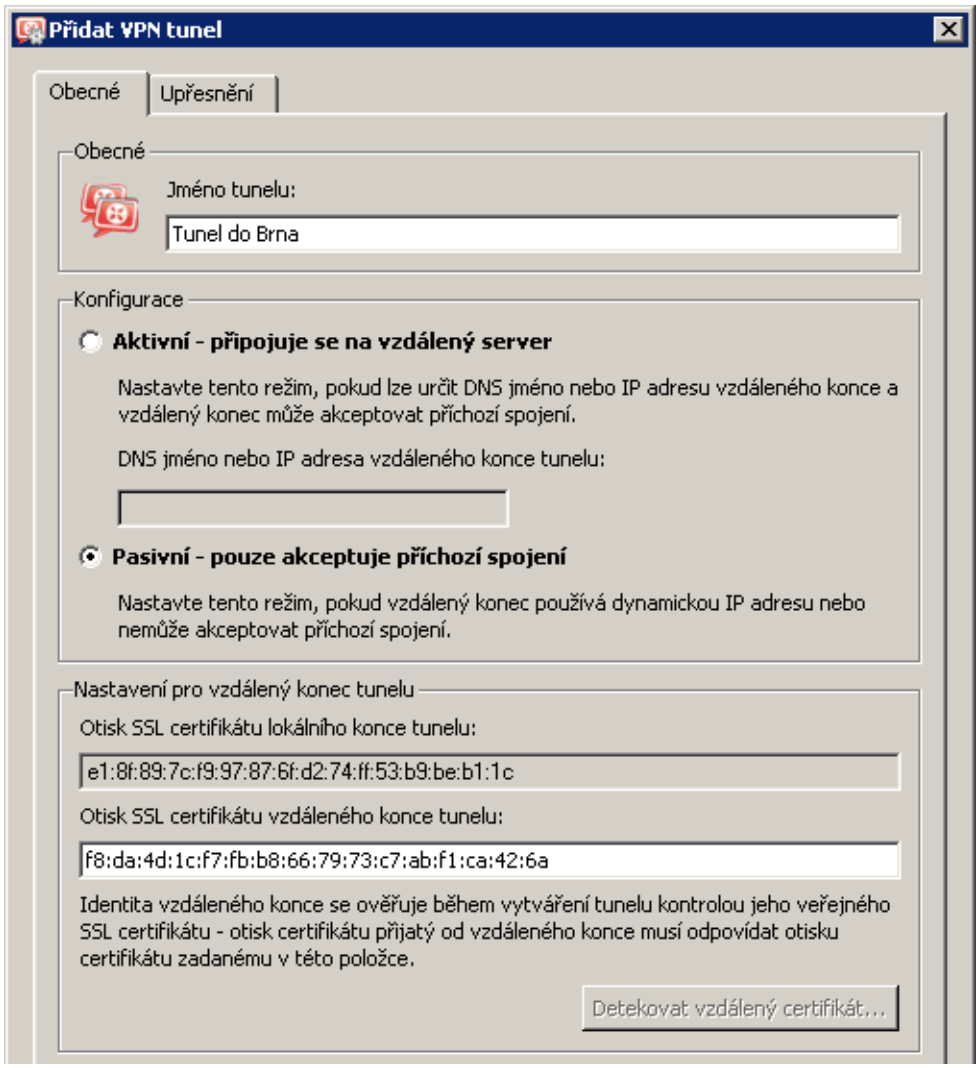


Obrázek 23.47 Pobočka Plzeň — definice VPN tunelu do centrály



Obrázek 23.48 Pobočka Plzeň — nastavení směrování pro tunel do centrály

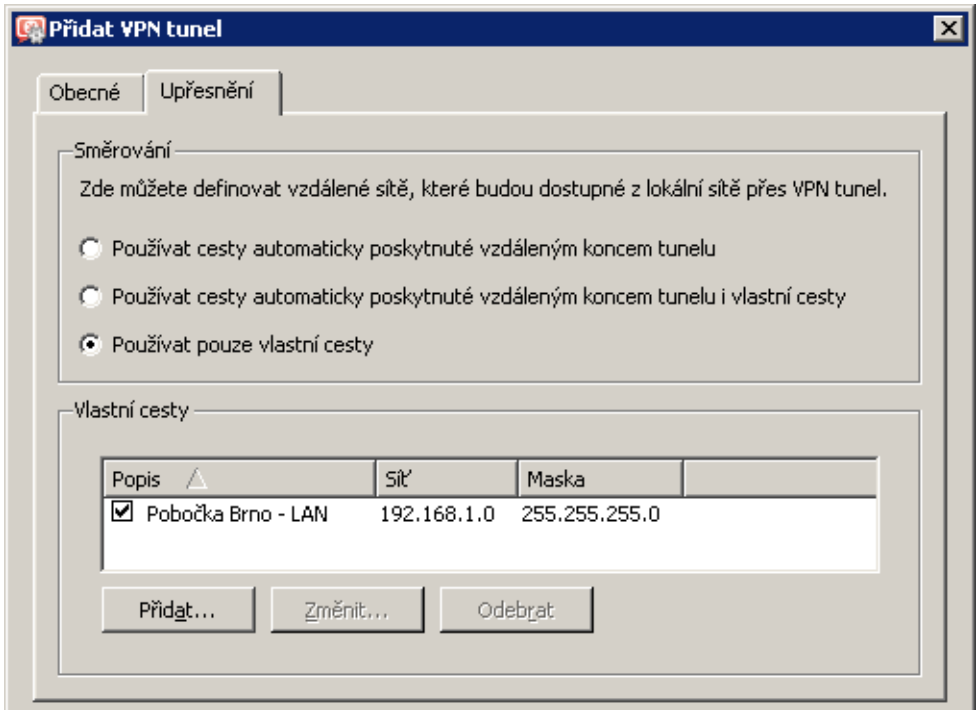
6. Vytvoříme pasivní konec tunelu do pobočky *Brno*. Jako otisk vzdáleného SSL certifikátu zadáme otisk certifikátu VPN serveru v pobočce *Brno*.



Obrázek 23.49 Pobočka Plzeň — definice VPN tunelu do pobočky Brno

V záložce *Upřesnění* zvolíme *Používat pouze vlastní cesty* a nastavíme cesty do lokálních sítí v pobočce *Brno*.

7. Do komunikačního pravidla *Lokální komunikace* přidáme vytvořené VPN tunely. Zároveň můžeme z tohoto pravidla odstranit nevyužité rozhraní *Dial-In* a skupinu *VPN klienti* (předpokládejme, že všichni VPN klienti se budou připojovat k serveru centrály).



Obrázek 23.50 Pobočka Plzeň — nastavení směrování pro tunel do pobočky Brno

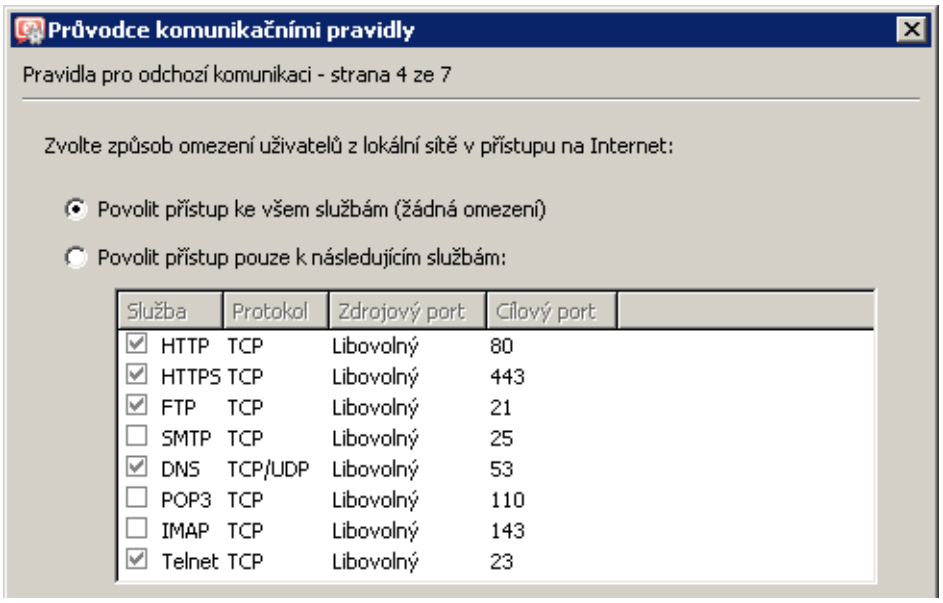
Jméno	Zdroj	Cíl	Služba	Akce
Služba Kerio VPN	Internet	Firewall	Kerio VPN	✓
Lokální komunikace	Firewall Všichni VPN klienti Tunel do Brna Tunel do centrály Důvěryhodné / lokální	Firewall Všichni VPN klienti Tunel do Brna Tunel do centrály Důvěryhodné / lokální	Libovolný	✓
Komunikace firewallu	Firewall	Libovolný	Libovolný	✓

Obrázek 23.51 Pobočka Plzeň — výsledná komunikační pravidla

Konfigurace v pobočce Brno

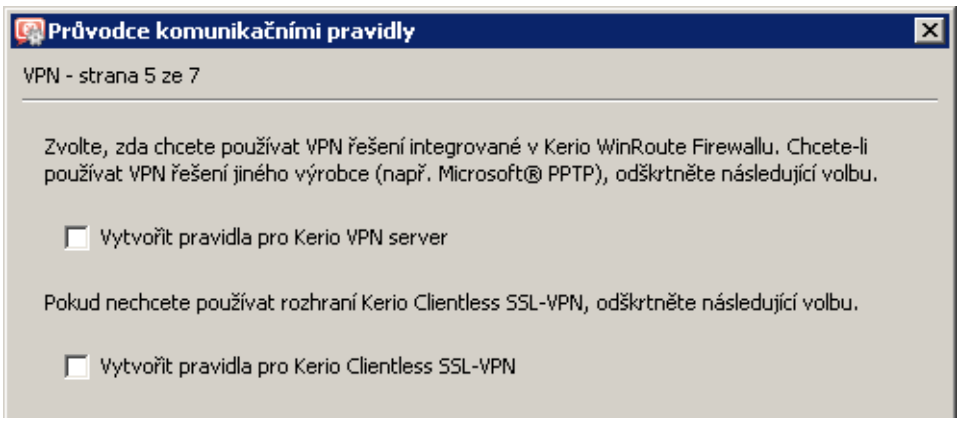
1. Na výchozí bránu sítě pobočky nainstalujeme *WinRoute* (verze `6.1.0` nebo vyšší).

2. Ve *WinRoute* nastavíme základní komunikační pravidla pomocí *Průvodce komunikačními pravidly* (viz kapitola 7.1). Pro jednoduchost předpokládejme, že nebudeme omezovat přístup z lokální sítě do Internetu, tzn. ve 4. kroku průvodce povolíme přístup ke všem službám.



Obrázek 23.52 Pobočka Brno — přístup z lokální sítě do Internetu bez omezení

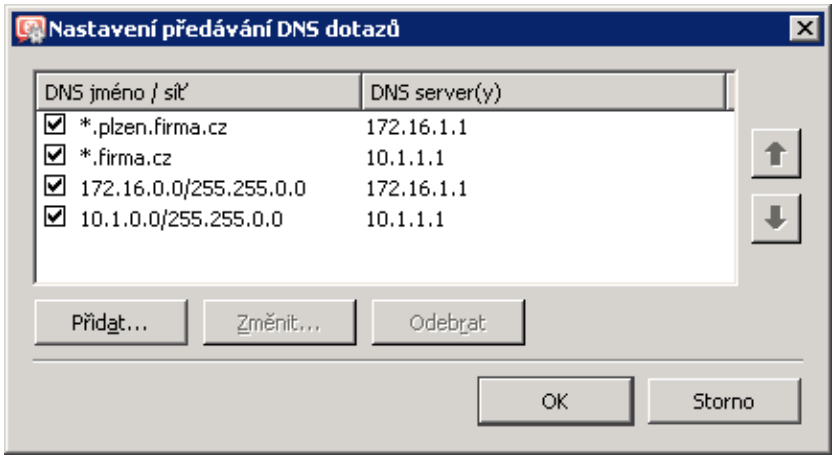
Vytvářet pravidla pro *Kerio VPN server* a *Kerio Clientless SSL-VPN* v tomto případě nemá smysl (server má dynamickou veřejnou IP adresu). V 5. kroku průvodce proto ponecháme obě volby vypnuté.



Obrázek 23.53 Pobočka Brno — výchozí pravidla pro Kerio VPN nebudou vytvořena

3. Nastavíme DNS (resp. upravíme nastavení DNS):

   - V konfiguraci modulu *DNS* ve *WinRoute* povolíme službu *DNS forwarder* (předávání DNS dotazů jiným serverům).
   - Zapneme volbu *Použít nastavení pro předávání DNS dotazů* a definujeme pravidla pro jména v doménách `firma.cz` a `plzen.firma.cz`. Jako DNS server pro předávání dotazů uvedeme IP adresu vnitřního rozhraní počítače s *WinRoute* na protější straně tunelu (tj. rozhraní připojeného do lokální sítě na protější straně).



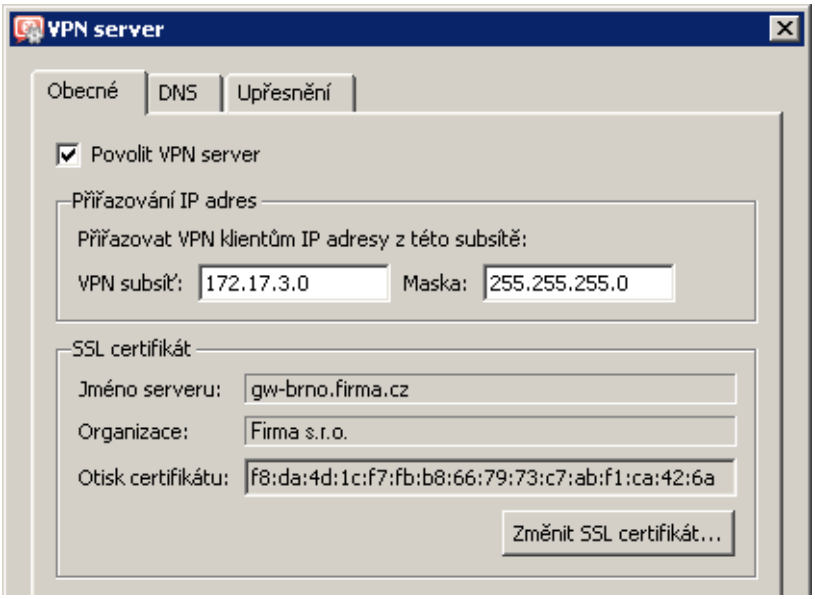
Obrázek 23.54 Pobočka Brno — nastavení předávání DNS dotazů

   - Na rozhraní počítače s *WinRoute* připojeném do lokální sítě *LAN 1* nastavíme jako upřednostňovaný (primární) DNS server IP adresu tohoto rozhraní (tj. `172.16.1.1`). Na rozhraní připojeném do lokální sítě *LAN 2* není třeba DNS nastavovat.
   - Na ostatních počítačích rovněž nastavíme jako upřednostňovaný (primární) DNS server IP adresu `172.16.1.1`.

4. Povolíme VPN server, případně nastavíme jeho SSL certifikát (nemáme-li certifikát vystavený důvěryhodnou certifikační autoritou, vytvoříme certifikát podepsaný sám sebou).

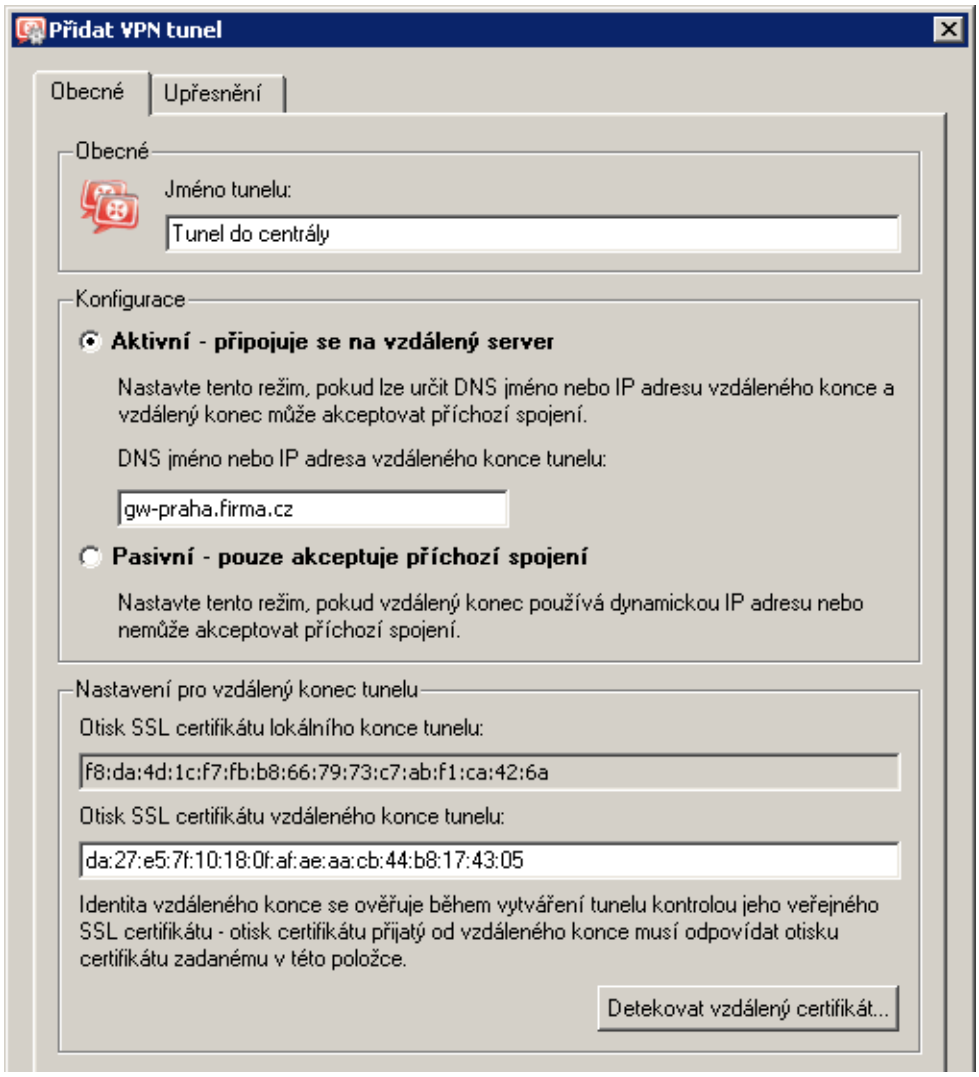
   Poznámka: V položkách *VPN subsíť* a *Maska* je nyní uvedena automaticky vybraná volná subsíť. Zkontrolujeme, zda tato subsíť nekoliduje s žádnou subsítí v centrále a na pobočkách, případně zadáme jinou (volnou) subsíť.

   Podrobnosti o konfiguraci VPN serveru viz kapitola 23.1.



Obrázek 23.55 Pobočka Brno — konfigurace VPN serveru

5. Vytvoříme aktivní konec VPN tunelu připojující se k serveru centrály (`praha.firma.cz`). Jako otisk vzdáleného SSL certifikátu zadáme otisk certifikátu VPN serveru v centrále.

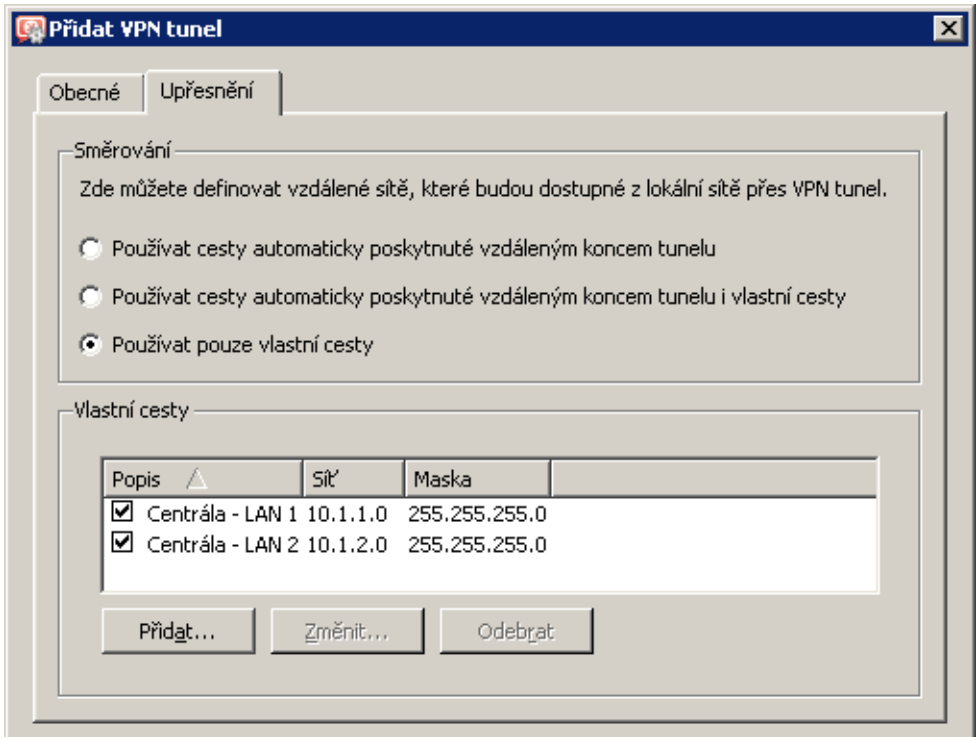


Obrázek 23.56 Pobočka Brno — definice VPN tunelu do centrály

V záložce *Upřesnění* zvolíme *Používat pouze vlastní cesty* a nastavíme cesty do lokálních sítí v *centrále*.

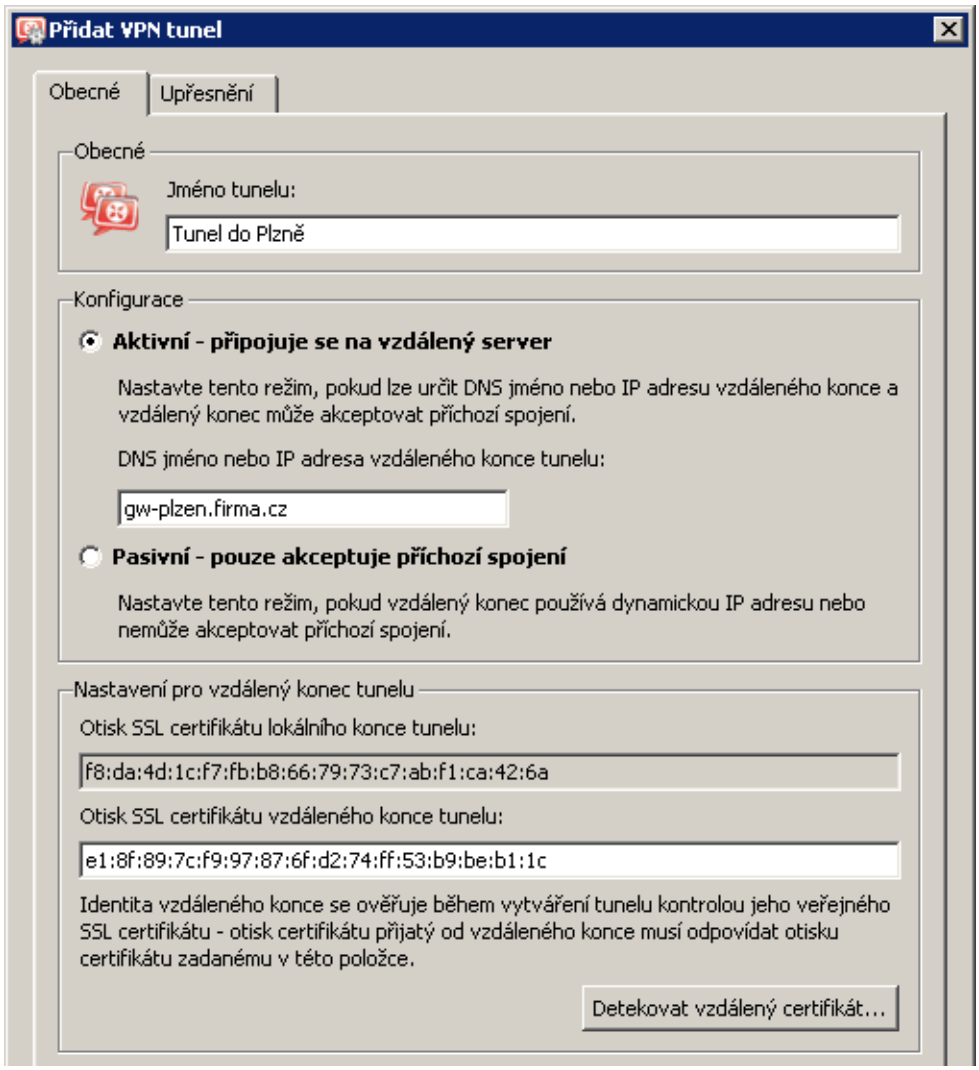
V tomto okamžiku by mělo dojít ke spojení — navázání tunelu. Je-li spojení úspěšné, zobrazí se u obou konců tunelu ve sloupci *Informace o adaptéru* stav *Připojeno*. Nedojde-li k navázání spojení, doporučujeme prověřit nastavení komunikačních pravidel a dostupnost vzdáleného serveru — v našem příkladu můžeme na serveru pobočky *Brno* zadat příkaz

```
ping gw-praha.firma.cz
```



Obrázek 23.57 Pobočka Brno — nastavení směrování pro tunel do centrály

6. Vytvoříme aktivní konec tunelu do pobočky *Plzeň* (server `gw-plzen.firma.cz`). Jako otisk vzdáleného SSL certifikátu zadáme otisk certifikátu VPN serveru v pobočce *Plzeň*.

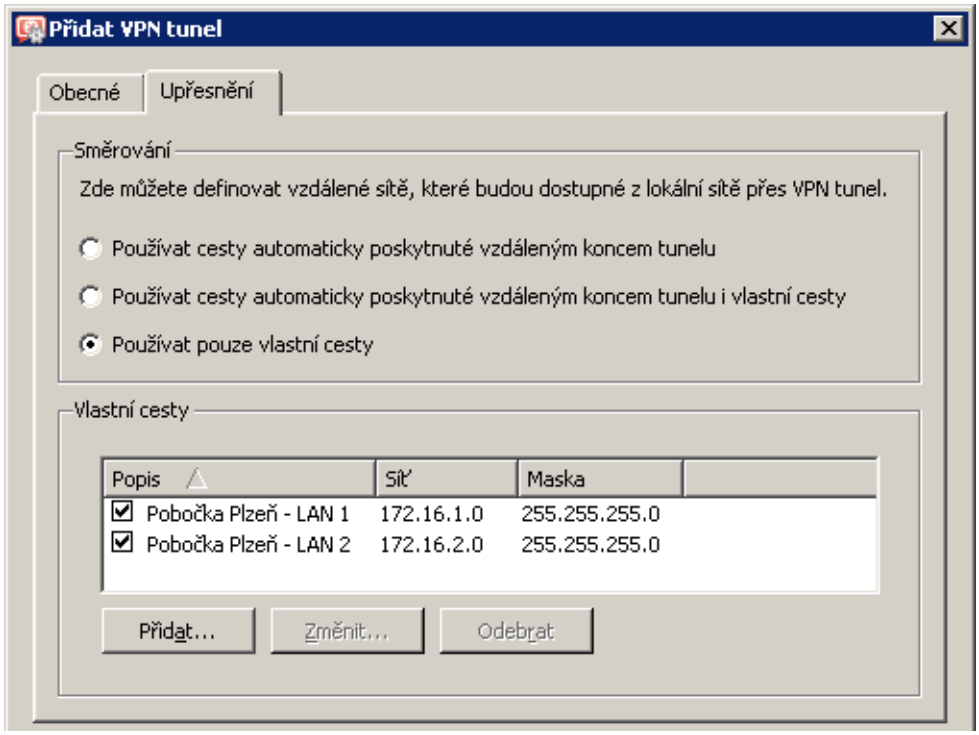


Obrázek 23.58 Pobočka Brno — definice VPN tunelu do pobočky Plzeň

V záložce *Upřesnění* zvolíme *Používat pouze vlastní cesty* a nastavíme cesty do lokálních sítí v pobočce *Plzeň*.

Podobně jako v předchozím kroku zkontrolujeme, zda došlo k navázání tunelu, a prověříme dostupnost vzdálených privátních sítí (tj. lokálních sítí v pobočce *Plzeň*).

7. Do komunikačního pravidla *Lokální komunikace* přidáme vytvořené VPN tunely. Zároveň můžeme z tohoto pravidla odstranit nevyužité rozhraní *Dial-In* a skupinu *VPN klienti* (do této pobočky se žádní VPN klienti připojovat nemohou).



Obrázek 23.59 Pobočka Brno — nastavení směrování pro tunel do pobočky Plzeň

Jméno	Zdroj	Cíl	Služba	Akce
Služba Kerio VPN	Internet	Firewall	Kerio VPN	✓
Lokální komunikace	Firewall Všichni VPN klienti Tunel do centrály Tunel do Plzně Důvěryhodné / lokální	Firewall Všichni VPN klienti Tunel do centrály Tunel do Plzně Důvěryhodné / lokální	Libovolný	✓
Komunikace firewallu	Firewall	Libovolný	Libovolný	✓

Obrázek 23.60 Pobočka Brno — výsledná komunikační pravidla

Test funkčnosti VPN

Konfigurace VPN je dokončena. Nyní doporučujeme z každé lokální sítě vyzkoušet dostupnost počítačů v ostatních vzdálených sítích (na protějších stranách jednotlivých tunelů).

Jako testovací nástroj lze použít např. příkazy operačního systému `ping` nebo `tracert`.

Kapitola 24

Kerio Clientless SSL-VPN (Windows)

Kerio Clientless SSL-VPN (dále jen „*SSL-VPN*“) je speciální rozhraní umožňující zabezpečený vzdálený přístup prostřednictvím WWW prohlížeče ke sdíleným prostředkům (souborům a složkám) v síti, kterou *WinRoute* chrání. Toto rozhraní je k dispozici pouze ve *WinRoute* na operačním systému *Windows*.

Rozhraní *SSL-VPN* je do jisté míry alternativou k aplikaci *Kerio VPN Client* (viz kapitola 23). Jeho základní výhodou je možnost okamžitého přístupu do vzdálené sítě odkudkoliv bez instalace speciální aplikace a jakékoliv konfigurace (odtud označení *clientless* — „bez klienta“). Naopak nevýhodou je netransparentní přístup do sítě. *SSL-VPN* je v podstatě obdobou systémového nástroje *Místa v síti* (*My Network Places*), neumožňuje přistupovat k WWW serverům a dalším službám ve vzdálené síti.

SSL-VPN je vhodné použít pro okamžitý přístup ke sdíleným souborům ve vzdálené síti všude tam, kde z nějakého důvodu nemůžeme nebo nechceme použít aplikaci *Kerio VPN Client*.

Tato kapitola popisuje konfigurační úkony nutné pro zajištění správné funkce rozhraní *SSL-VPN*. Samotné rozhraní *SSL-VPN* je podrobně popsáno v manuálu *Kerio WinRoute Firewall — Příručka uživatele*.

24.1 Konfigurace SSL-VPN ve WinRoute

Podmínky pro správnou funkci rozhraní SSL-VPN

Pro správnou funkci rozhraní *SSL-VPN* musejí být splněny tyto podmínky:

1. Počítač s *WinRoute* musí být členem příslušné domény (*Windows NT* nebo *Active Directory*).

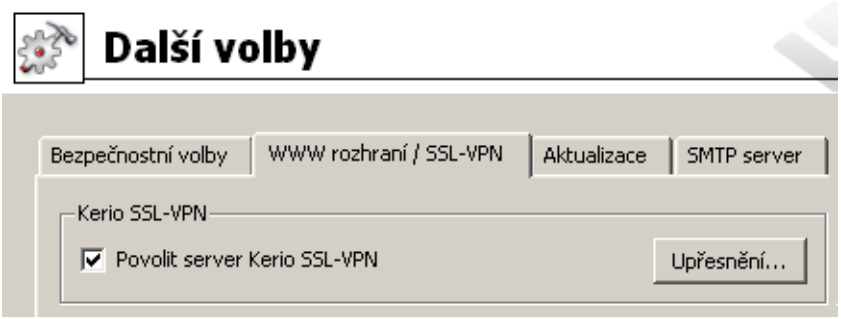
2. Uživatelské účty, které budou používány k přihlášení do *SSL-VPN*, musí být ověřovány v této doméně (nelze použít lokální ověřování). Z toho vyplývá, že rozhraní *SSL-VPN* nelze použít pro přístup ke sdíleným prostředkům ve více doménách ani k prostředkům na počítačích, které nejsou členy žádné domény.

3. Uživatelům, kteří mají mít do rozhraní *SSL-VPN* přístup, musí být ve *WinRoute* uděleno právo používat *Clientless SSL-VPN* (viz kapitola 15.2).

4. Je-li *WinRoute* nainstalován na doménovém serveru, pak musí být příslušným uživatelům povoleno lokální přihlášení na tento server. Lokální přihlášení lze povolit v zásadách zabezpečení doménového serveru (*Domain Controller Security Policy*). Bližší informace naleznete v Databázi znalostí (v angličtině).

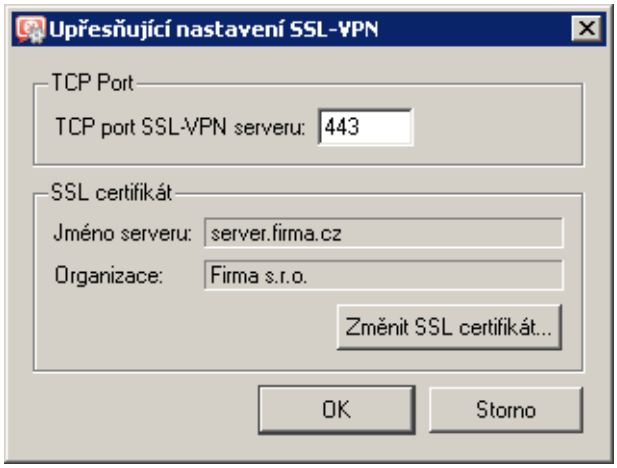
Nastavení parametrů rozhraní SSL-VPN

Rozhraní *SSL-VPN* lze zapnout nebo vypnout v sekci *Konfigurace* → *Další volby*, záložka *WWW rozhraní* → *SSL-VPN*.



Obrázek 24.1 Konfigurace rozhraní SSL-VPN

Tlačítko *Upřesnění* umožňuje nastavit port a SSL certifikát rozhraní *SSL-VPN*.



Obrázek 24.2 Nastavení portu a SSL certifikátu pro SSL-VPN

Výchozím portem pro rozhraní *SSL-VPN* je port `443` (jedná se o standardní port služby *HTTPS*).

Tlačítkem *Změnit SSL certifikát* lze vytvořit nový certifikát pro službu *SSL-VPN* nebo importovat certifikát vystavený důvěryhodnou certifikační autoritou. Vytvořený certifikát bude uložen do souboru `sslvpn.crt` a odpovídající privátní klíč do souboru `sslvpn.key`. Postup vytvoření a importu certifikátu je stejný jako v případě WWW rozhraní *WinRoute* nebo VPN serveru a je podrobně popsán v kapitole 11.1.

Tip

Certifikát vystavený certifikační autoritou na konkrétní jméno serveru lze použít zároveň pro WWW rozhraní, VPN server i službu *SSL-VPN* — není nutné mít tři různé certifikáty.

Povolení přístupu z Internetu

Přístup z Internetu k rozhraní *SSL-VPN* je třeba explicitně povolit definicí komunikačního pravidla povolujícího připojení ke službě *HTTPS* na firewallu. Podrobnosti viz kapitola 7.4.

Obrázek 24.3 Komunikační pravidlo povolující přístup k rozhraní SSL-VPN

Poznámka: V případě změny portu rozhraní *SSL-VPN* je třeba upravit také položku *Služba* v tomto pravidle!

Antivirová kontrola

Je-li ve *WinRoute* aktivní alespoň jeden antivirus (viz kapitola 13), pak může být prováděna antivirová kontrola souborů přenášených rozhraním *SSL-VPN*.

Ve výchozí konfiguraci se provádí pouze kontrola souborů nahrávaných na počítače ve vzdálené privátní síti.. Na soubory stahované ze vzdálené sítě na lokální počítač se z důvodu rychlosti antivirová kontrola neaplikuje (soubory z privátní sítě jsou považovány za důvěryhodné). Nastavení antivirové kontroly lze změnit v konfiguraci antivirů — viz kapitola 13.5.

24.2 Použití rozhraní SSL-VPN

Pro přístup k rozhraní lze využít většinu běžných grafických WWW prohlížečů (doporučujeme *Internet Explorer* verze 6.0 nebo *Firefox/SeaMonkey* s jádrem od verze 1.3). Do prohlížeče zadáme URL ve tvaru

```
https://server/
```

kde `server` je DNS jméno nebo IP adresa počítače s *WinRoute*. Používá-li *SSL-VPN* jiný port než standardní port služby *HTTPS* (443), pak je třeba v URL uvést také příslušný port — např.:

```
https://server:12345/
```

Po připojení k serveru se zobrazí přihlašovací stránka rozhraní *SSL-VPN* v jazyce dle nastavení prohlížeče. Není-li k dispozici lokalizace pro žádný z jazyků preferovaných v prohlížeči, bude použita angličtina.

Kapitola 25

Specifické konfigurace a řešení problémů

V této kapitole uvádíme popis pokročilejších funkcí a specifických konfigurací firewallu. Rovněž zde naleznete praktické návody k vyřešení problémů, které mohou vzniknout při nasazení a používání *WinRoute* ve vaší síti.

25.1 Zálohování a přenos konfigurace

V případě nutnosti přeinstalování operačního systému firewallu (např. při výměně hardware) je možné zálohovat konfiguraci *WinRoute* včetně lokálních uživatelských účtů a (volitelně) SSL certifikátů. Tuto zálohu pak lze použít pro obnovení původní konfigurace v nové instalaci *WinRoute*. Tímto postupem lze ušetřit značné množství času a vyhnout se opakovanému řešení již vyřešených problémů.

Chceme-li provést export nebo import konfigurace, přihlásíme se do rozhraní *Web Administration* (viz kapitola 3) a přímo na úvodní stránce klikneme na příslušný odkaz.

Export konfigurace

Při exportu konfigurace bude vytvořen balík ve formátu *.tgz* (archiv *tar* komprimovaný *gzip*) obsahující všechny důležité konfigurační soubory *WinRoute*. Volitelně mohou být do archivu přidány také SSL certifikáty WWW rozhraní, VPN serveru a serveru *SSL-VPN*. Exportovaná konfigurace neobsahuje licenčním klíč *WinRoute*.

Import konfigurace

Při importu konfigurace stačí vyhledat nebo zadat cestu k příslušnému souboru s exportovanou konfigurací (ve formátu *.tgz*).

Pokud po exportu došlo ke změně síťových rozhraní firewallu (např. výměna vadného síťového adaptéru) nebo pokud importujeme konfiguraci z jiného počítače, pak se *WinRoute* pokusí spárovat síťová rozhraní z importované konfigurace se skutečnými rozhraními. Toto párování lze případně upravit podle potřeby — ke každému síťovému rozhraním z importované konfigurace můžeme přiřadit vybrané rozhraní firewallu, případně nepřiřadit žádné rozhraní.

Pokud nelze síťová rozhraní jednoznačně spárovat, je potřeba po dokončení importu konfigurace zkontrolovat a případně upravit nastavení skupin rozhraní (viz kapitola 5) a/nebo komunikačních pravidel (viz kapitola 7).

25.2 Konfigurační soubory

V této kapitole uvádíme přehledný popis konfiguračních a stavových souborů *WinRoute*. Tyto informace mohou pomoci např. při řešení specifických problémů ve spolupráci s technickou podporou *Kerio Technologies*.

Pro zálohování a obnovení konfigurace firewallu doporučujeme použít nástroje pro export a import konfigurace popsané v kapitole 25.1!

Konfigurační soubory

Veškeré konfigurační informace *WinRoute* jsou uloženy v adresáři, kde je *WinRoute* nainstalován

(typicky `C:\Program Files\Kerio\WinRoute Firewall`).

Jedná se o tyto soubory:

winroute.cfg
: Hlavní konfigurační soubor.

UserDB.cfg
: Informace o uživatelských účtech a skupinách.

host.cfg
: Parametry pro ukládání konfigurace, uživatelských účtů, databáze DHCP serveru, statistik atd.

logs.cfg
: Konfigurace záznamů.

Poznámka: 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.

Za konfigurační informace lze považovat rovněž soubory v těchto adresářích:

dbSSL
: Automaticky generovaný SSL certifikát pro komunikaci mezi *WinRoute Firewall Engine* a *Administration Console*.
Podrobnosti o komunikaci mezi *WinRoute Firewall Engine* a *Administration Console* naleznete v manuálu *Kerio Administration Console — Nápověda* (http://www.kerio.cz/cz/firewall/manual).

sslcert
: SSL certifikáty pro všechny komponenty využívající SSL pro zabezpečení komunikace (tj. WWW rozhraní, VPN server a rozhraní *Clientless SSL-VPN*).

license
Pokud byl *WinRoute* již zaregistrován, obsahuje adresář `license` soubor s licenčním klíčem (i v případě registrované zkušební verze). Není-li *WinRoute* dosud zaregistrován, pak je adresář `license` prázdný.

Stavové soubory

WinRoute rovněž vytváří několik souborů a adresářů, do kterých ukládá určité stavové informace.

Soubory:

dnscache.cfg
DNS záznamy uložené v cache modulu *DNS* (viz kapitola 8.1).

leases.cfg
IP adresy přidělené DHCP serverem.
Tento soubor obsahuje všechny informace, které se zobrazují v sekci *Konfigurace* → *DHCP server*, záložka *Přidělené adresy* (viz kapitola 8.2).

stats.cfg
Data statistik rozhraní (viz kapitola 20.2) a statistik uživatelů (viz kapitola 20.1).

vpnleases.cfg
IP adresy přidělené VPN klientům (viz kapitola 23.2).

Adresáře:

logs
Do adresáře `logs` ukládá *WinRoute* všechny záznamy (viz kapitola 22).

star
Adresář `star` obsahuje kompletní databázi pro statistiky zobrazované ve WWW rozhraní *WinRoute*.

Manipulace s konfiguračními soubory

Před jakoukoliv manipulací s konfiguračními soubory (zálohováním, obnovováním apod.) 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 z operační paměti.

25.3 Automatické ověřování uživatelů pomocí NTLM

WinRoute podporuje automatické ověřování uživatelů z WWW prohlížečů metodou NTLM. Je-li uživatel přihlášen do domény, nemusí pro ověření na firewallu zadávat znovu své uživatelské jméno a heslo.

Tato kapitola podrobně popisuje podmínky, které musí být splněny, a konfigurační kroky, které je nutné provést, aby NTLM ověřování z klientských počítačů fungovalo správně.

Obecné podmínky

Ověřování pomocí NTLM funguje správně pouze za dodržení následujících podmínek:

1. *WinRoute Firewall Engine* musí být spouštěn jako služba nebo musí být spouštěn pod účtem uživatele, který má administrátorská práva k počítači, na kterém je *WinRoute* nainstalován.

2. Server (tj. počítač s *WinRoute*) musí být členem příslušné domény *Windows NT* nebo *Active Directory* (*Windows 2000/2003/2008*).

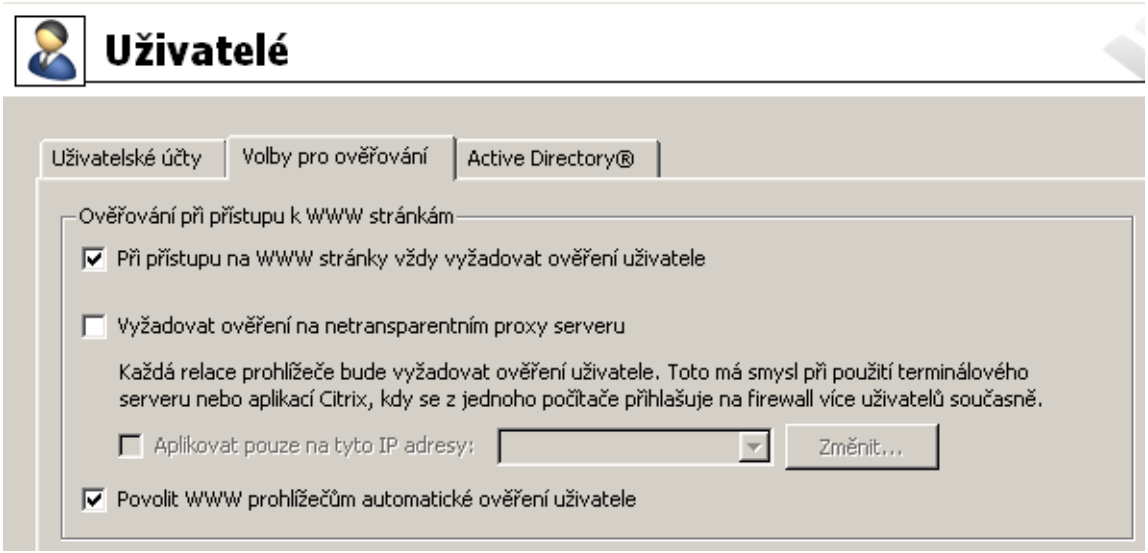
3. Klientský počítač musí být rovněž členem této domény.

4. Uživatel na klientském počítači se musí přihlašovat do této domény (tzn. nelze použít lokální uživatelský účet).

5. Příslušný uživatelský účet ve *WinRoute* musí být ověřován v doméně *Active Directory* nebo *Windows NT* (viz kapitola 15.1). NTLM nelze použít pro uživatele ověřované interně *WinRoute*.

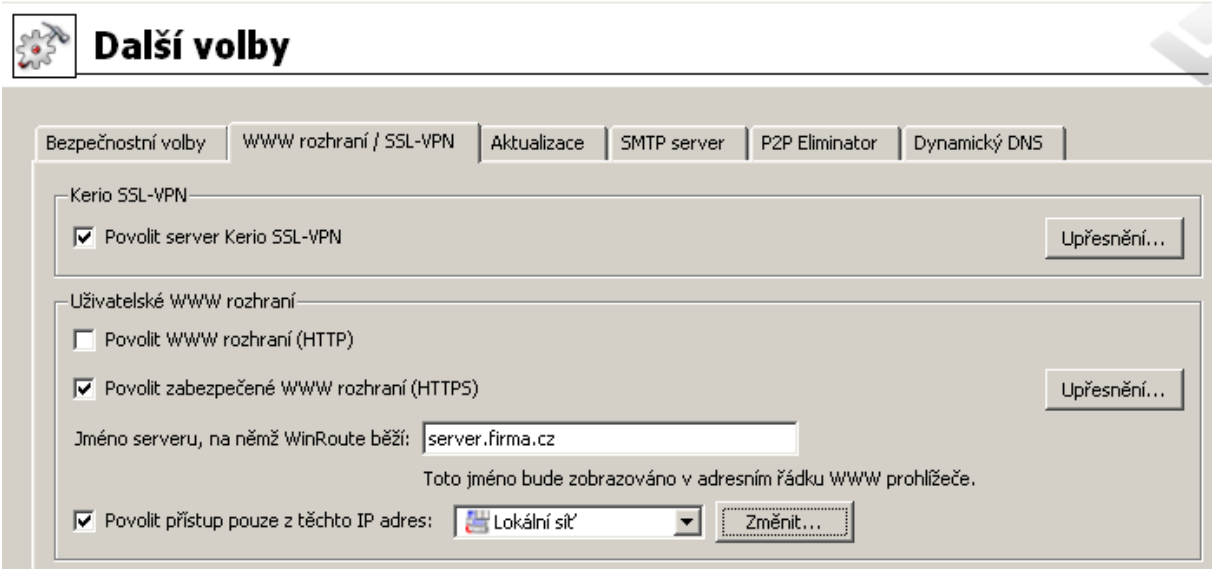
Konfigurace WinRoute

V sekci *Uživatelé* → *Volby pro ověřování* musí být povoleno automatické ověřování uživatelů z WWW prohlížečů. Zároveň by mělo být vyžadováno ověřování uživatelů při přístupu na WWW stránky (jinak NTLM ověřování z prohlížečů postrádá smysl).



Obrázek 25.1 NTLM — nastavení ověřování uživatelů

V konfiguraci WWW rozhraní *WinRoute* musí být nastaveno platné DNS jméno serveru, na němž *WinRoute* běží (podrobnosti viz kapitola 11.1).



Obrázek 25.2 Nastavení parametrů WWW rozhraní WinRoute

Poznámka: V edici *Software Appliance / VMware Virtual Appliance* se jméno serveru nastavuje v záložce *Systémová konfigurace* (viz kapitola 16.1).

WWW prohlížeče

Pro správnou funkci NTLM ověřování je třeba použít WWW prohlížeč, který tuto metodu ověřování podporuje. V současné době lze použít tyto prohlížeče:

- *Internet Explorer* verze *5.01* a vyšší
- *Firefox nebo SeaMonkey* s jádrem *Mozilla 1.3* nebo novějším

Průběh NTLM ověření

Z pohledu uživatele probíhá NTLM ověření na firewallu odlišně podle typu použitého WWW prohlížeče.

Internet Explorer

NTLM ověření proběhne bez interakce uživatele.

Pouze v případě, že se NTLM ověření nezdaří (např. pokud ve *WinRoute* neexistuje uživatelský účet pro uživatele přihlášeného na klientském počítači), se zobrazí přihlašovací dialog.

Upozornění

Jedním z důvodů selhání NTLM ověření může být neplatné přihlašovací jméno/heslo uložené ve *Správci hesel* systému *Windows* (*Ovládací panely* → *Uživatelské účty* → *Upřesnění* → *Správce hesel*) pro příslušný server (tj. počítač s *WinRoute*). *Internet Explorer* v takovém případě odešle na server uložené přihlašovací údaje namísto NTLM ověření aktuálně přihlášeného uživatele. Při problémech s NTLM ověřováním doporučujeme ze *Správce hesel* odstranit všechna uložená jména/hesla pro server, na kterém je *WinRoute* nainstalován.

Firefox/SeaMonkey

Prohlížeč zobrazí přihlašovací dialog. Ve výchozím nastavení prohlížeče se z bezpečnostních důvodů automatické ověření uživatele neprovádí. Toto chování prohlížeče lze změnit úpravou konfiguračních parametrů — viz níže.
Pokud se ověření nezdaří, dojde v případě přímého připojení k přesměrování prohlížeče na přihlašovací stránku firewallu (viz kapitola 11.2). V případě použití proxy serveru se opět zobrazí přihlašovací dialog.

Poznámka: Pokud se NTLM ověření uživatele z nějakého důvodu nezdaří, zapíší se podrobné informace o této události do záznamu *error* (viz kapitola 22.8).

Nastavení parametrů prohlížeče Firefox/SeaMonkey

Změnou konfiguračních parametrů prohlížeče lze povolit automatické ověření metodou NTLM — bez zobrazení přihlašovacího dialogu. Postup je následující:

1. Do adresního řádku prohlížeče zadáme: `about:config`. Zobrazí se seznam konfiguračních parametrů.

2. Nastavíme příslušný konfigurační parametr:

   - V případě přímého připojení (v prohlížeči není nastaven proxy server):
     Vyhledáme parametr `network.automatic-ntlm-auth.trusted-uris`. Jako hodnotu tohoto parametru nastavíme jméno počítače s *WinRoute* (např. `server` nebo `server.firma.cz`). Toto jméno musí korespondovat se jménem serveru nastaveným v sekci *Konfigurace* → *Další volby* → *WWW rozhraní* (viz kapitola 11.1).
     Poznámka: V tomto parametru *nelze* použít IP adresu!
   - V případě použití proxy serveru ve *WinRoute*:
     Vyhledáme parametr `network.automatic-ntlm-auth.allow-proxies` a nastavíme jej na hodnotu `true`.

   Změny konfiguračních parametrů jsou účinné ihned — prohlížeč není třeba restartovat.

25.4 FTP přes proxy server ve WinRoute

Proxy server ve *WinRoute* verze *6.0.2* a vyšší (viz kapitola 8.4) podporuje protokol FTP. Při použití tohoto způsobu přístupu k FTP serverům je však třeba mít na paměti určitá specifika,

která vyplývají jednak z principu technologie proxy a jednak z vlastností proxy serveru ve *WinRoute*.

1. FTP klient musí umožňovat nastavení proxy serveru. Toto umožňují např. WWW prohlížeče (*Internet Explorer*, *Firefox/SeaMonkey*, *Opera* apod.), *Total Commander* (dříve *Windows Commander*), *CuteFTP* atd.

   Terminálový FTP klienti (např. příkaz `ftp` v operačním systému *Windows* nebo *Linux*) nastavení proxy serveru neumožňují a nelze je tedy v tomto případě použít.

2. Proxy server používá pro přístup k FTP serveru pasivní režim FTP. Je-li FTP server chráněn firewallem bez podpory FTP (což není případ *WinRoute*), nebude možné se na tento server přes proxy připojit.

3. Nastavení režimu FTP v klientovi nemá při použití proxy serveru žádný smysl. Mezi klientem a proxy serverem se navazuje vždy pouze jedno síťové spojení, kterým se protokol FTP „tuneluje“.

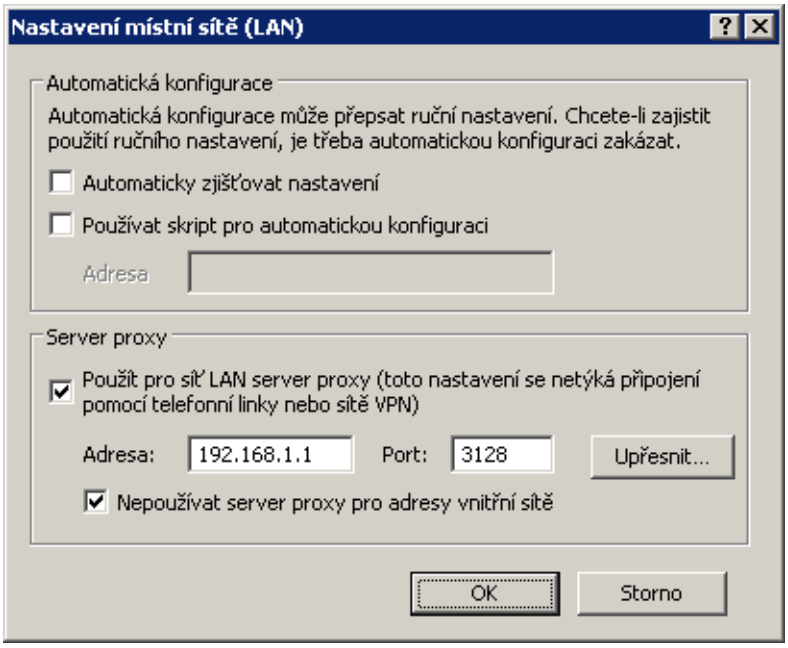
Poznámka: FTP přes proxy server doporučujeme používat pouze v případech, kdy nelze využít přímý přístup do Internetu (viz kapitola 8.4).

Příklad konfigurace klienta: WWW prohlížeč

WWW prohlížeče umožňují nastavit proxy server buď globálně, nebo pro jednotlivé protokoly. Jako příklad uvedeme nastavení prohlížeče *Internet Explorer 6.0* (konfigurace ostatních prohlížečů je téměř identická).

1. V hlavním menu prohlížeče zvolíme *Nástroje* → *Možnosti Internetu*, vybereme záložku *Připojení* a stiskneme tlačítko *Nastavení místní sítě*.

2. Zapneme volbu *Použít pro síť LAN server proxy* a zadáme IP adresu a port proxy serveru. IP adresa proxy serveru je adresa rozhraní počítače s *WinRoute* připojeného do lokální sítě; výchozí port proxy serveru je `3128` (podrobnosti viz kapitola 8.4). Doporučujeme zapnout rovněž volbu *Nepoužívat server proxy pro adresy vnitřní sítě* — použití proxy pro lokální servery by zbytečně zpomalovalo komunikaci a zatěžovalo *WinRoute*.



Obrázek 25.3 Nastavení proxy serveru v prohlížeči Internet Explorer 6.0

Tip

Pro nastavení WWW prohlížečů můžeme s výhodou využít konfigurační skript, případně automatickou detekci nastavení. Podrobnosti viz kapitola 8.4.

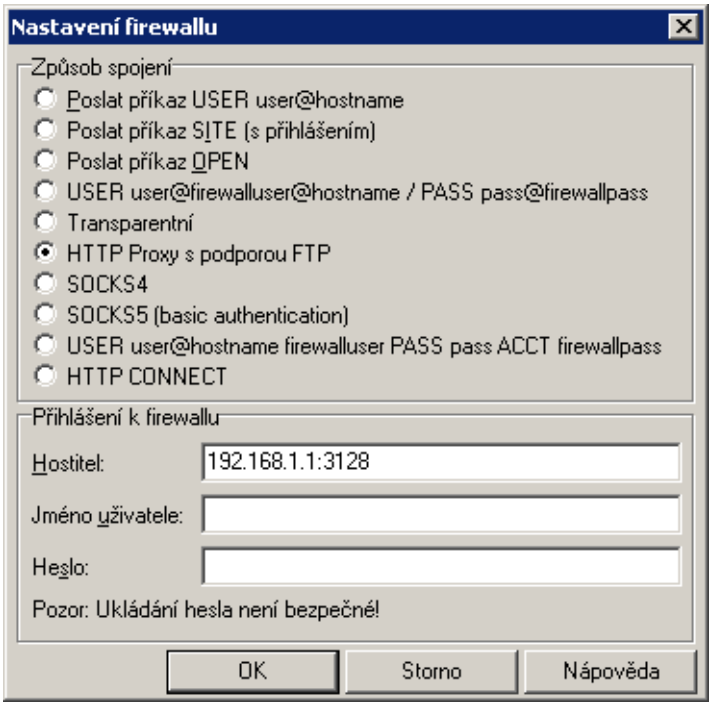
Poznámka: WWW prohlížeče jako FTP klienti umožňují pouze download souborů. Upload na FTP server pomocí WWW prohlížeče není možný.

Příklad konfigurace klienta: Total Commander

Total Commander umožňuje buď jednorázové připojení k FTP serveru (volba *Síť* → *FTP - nové připojení* v hlavním menu) nebo vytvoření záložky pro opakované připojení (volba *Síť* → *FTP - připojit se*). Proxy server je třeba nastavit pro každé FTP připojení (resp. pro každou záložku).

1. V dialogu pro FTP připojení zapneme volbu *Použít firewall (proxy server)* a stiskneme tlačítko *Změnit*.

2. V dialogu *Nastavení firewallu* zvolíme způsob spojení *HTTP Proxy s podporou FTP*. Do položky *Hostitel* zadáme IP adresu a port proxy serveru (oddělené dvojtečkou, bez mezer — např. `192.168.1.1:3128`). Položky *Jméno uživatele* a *Heslo* není třeba vyplňovat (*WinRoute* s těmito údaji nepracuje).



Obrázek 25.4 Nastavení proxy serveru pro FTP v Total Commanderu

Tip

Definovaný proxy server se automaticky uloží do seznamu proxy serverů pod určitým číslem. Při vytváření dalších FTP připojení pak stačí vybrat příslušný proxy server ze seznamu.

25.5 Internetové linky vytáčené na žádost

Při použití internetové linky vytáčené na žádost (viz kapitola 6.2) je třeba mít na paměti určité specifické vlastnosti tohoto typu připojení. Při nesprávné konfiguraci sítě a firewallu může docházet k tomu, že linka zůstává zavěšena i přesto, že v lokální síti vznikají požadavky na přístup do Internetu, nebo naopak dochází ke zdánlivě bezdůvodnému vytáčení linky.

Informace v této kapitole by měly pomoci k pochopení principu a vlastností funkce vytáčení linky na žádost a předejít tak uvedeným problémům.

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 — viz kapitola 6.2).

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 cílovou IP adresu 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.

Aby nedocházelo k nežádoucímu vytáčení linky, je vytočení linky povoleno pouze pro určité typy paketů. Linku mohou vytočit pouze UDP pakety nebo TCP pakety s příznakem *SYN* (navazování spojení). Vytáčení na žádost je zakázáno pro služby sítě *Microsoft Networks* (sdílení souborů a tiskáren atd.).

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.

Poznámka:

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. Pro vytáčení na žádost může být ve *WinRoute* nastavena vždy pouze jedna linka. *WinRoute* neumožňuje automatický výběr linky, která má být vytočena.

3. Linka může být také vytáčena na základě statické cesty ve směrovací tabulce (viz kapitola 18.1). 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 k 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 internetová linka 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 modul *DNS* ve *WinRoute* automatické vytočení linky, jestliže není schopen DNS dotaz sám vyřídit. Tato funkce je svázána s vytáčením na žádost.

   Poznámka: Bude-li DNS server 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 modul *DNS*, který dokáže v případě potřeby vytočit linku.

   Je-li v lokální síti doména založená na *Active Directory* (doménový server s operačním systémem *Windows Server 2000/2003/2008*), musí být použit *Microsoft* DNS server, 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 modulem *DNS*, protože by došlo ke kolizi portů.

   Z výše uvedeného vyplývá, že pokud má být připojení k Internetu realizováno vytáčenou linkou, *nemůže* být *WinRoute* nasazen na tentýž počítač, kde běží *Windows Server* s *Active Directory* a *Microsoft* DNS.

4. Je-li použit modul *DNS*, 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 rozhraních připojených do lokání sítě

nastavíme jako primární DNS server stejnou IP adresu, jaká je přiřazena příslušnému rozhraní.

5. *Proxy server* ve *WinRoute* (viz kapitola 8.4) dokáže vytáčet linku přímo. Uživateli se po dobu vytáčení linky zobrazí speciální stránka informující o průběhu vytáčení (stránka je v pravidelných intervalech obnovována). Po úspěšném vytočení linky dojde k automatickému přesměrování na požadovanou WWW stránku.

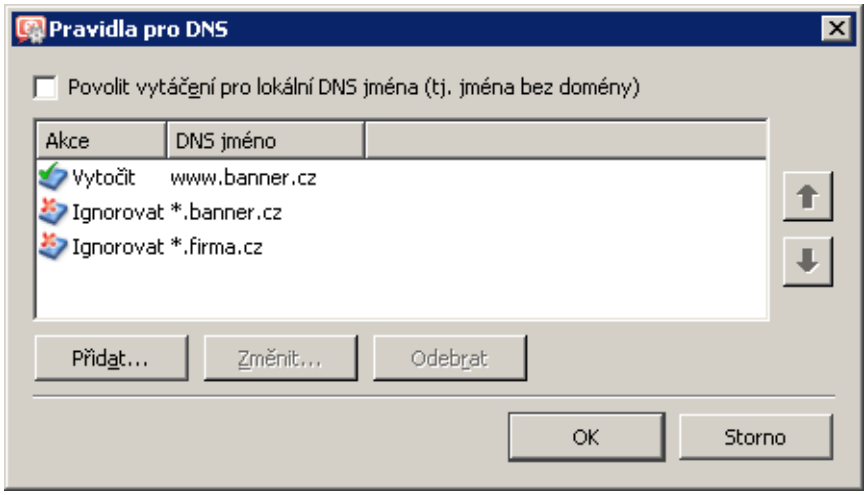
Nežádoucí vytáčení linky — použití pravidel pro vytáčení na žádost

Vytáčení na žádost může mít v určitých případech nepříjemný postranní efekt — nechtěné vytáčení linky, zdánlivě bez zjevné příčiny. V naprosté většině případů je to způsobeno DNS dotazy, které modul *DNS* 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. aktivní objekt na lokálně uložené HTML stránce či automatická aktualizace některého z instalovaných programů, ale také virus či trojský kůň.
- Modul *DNS* 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 — viz kapitola 8.1).

Poznámka: Nežádoucí komunikaci způsobující vytáčení linky je možné ve *WinRoute* blokovat komunikačními pravidly (viz kapitola 7.3). Primární snahou by ale vždy mělo být odstranit její příčinu (tj. např. provést antivirovou kontrolu příslušné stanice apod.).

Pro zamezení nežádoucího vytáčení linky na základě DNS dotazů umožňuje *WinRoute* definovat pravidla, které určují, zda se pro daná DNS jména smí vytočit linka či nikoliv. Tato pravidla lze nastavit po stisknutí tlačítka *Upřesnění* v sekci *Konfigurace* → *Rozhraní* (v režimu *Jedna internetová linka — vytáčení na žádost*).



Obrázek 25.5 Pravidla pro vytáčení na žádost na základě DNS dotazů

DNS jméno v pravidle může být zadáno úplné, nebo jeho začátek či konec doplněn znakem hvězdička (*). Hvězdička nahrazuje libovolný počet znaků.

Pravidla tvoří uspořádaný seznam, který 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 modul *DNS* v případě potřeby automaticky vytáčet.

Akce pro DNS jméno může být *Vytočit* nebo *Ignorovat*, tj. nevytáčet při dotazu na toto DNS jméno. 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 25.5).

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 modul *DNS* využívá). Modul *DNS* ve výchozím nastavení na tato jména nevytáčí, protože pokud není lokální jméno nalezeno v lokální DNS databázi, považuje se za neexistující.

V případě, kdy je primární server lokální domény umístěn mimo lokální síť, je třeba, aby modul *DNS* 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*). Ve všech ostatních případech doporučujeme ponechat tuto volbu vypnutou (opět může nastat nežádoucí efekt vytáčení linky zdánlivě bez příčiny).

Kapitola 26

Technická podpora

Společnost *Kerio Technologies* poskytuje na produkt *Kerio WinRoute Firewall* bezplatnou e-mailovou a telefonickou technickou podporu. Kontakty a další informace naleznete na stránce http://www.kerio.cz/cz/support. 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.

26.1 Informace pro technickou podporu

Požadavek na technickou podporu můžete zadat prostřednictvím kontaktního formuláře na WWW stránkách http://support.kerio.cz/.

Abychom vám mohli co nejlépe a nejrychleji pomoci, potřebujeme získat maximum informací o vaší konfiguraci a řešeném problému. Uveďte prosím (alespoň) následující informace:

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 *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 *Administration Console*.
- Je-li internetové připojení realizováno vytáčenou linkou, připojte se.
- V programu *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 *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.

Typ licence a licenční číslo

Uveďte prosím, zda vlastníte licenci na produkt *WinRoute* či zda se jedná o zkušební verzi (trial). Požadavky majitelů platných licencí jsou vyřizovány přednostně.

26.2 Testování betaverzí

V zájmu zvyšování kvality svých produktů uvolňuje společnost *Kerio Technologies* významnější verze svých produktů před oficiálním vydáním jako tzv. betaverze. Betaverze jsou verze, ve kterých se již nacházejí všechny plánované nové funkce, ale stále jsou ve fázi vývoje. Dobrovolní testeři těchto verzí mohou přispět k vylepšení produktu nebo odhalení chyb.

Pro vývoj produktu je důležitá zpětná vazba od testerů (bez zpětných informací o nalezených chybách a problémech nemá testování betaverzí smysl). Betaverze *WinRoute* proto obsahují rozšíření umožňující testerům snadnou komunikaci se společností *Kerio Technologies*.

Bližší informace o betaverzích a možnostech jejich testování naleznete na adrese http://www.kerio.cz/cz/betas.

Příloha A

Právní doložka

Microsoft®, *Windows*®, *Windows NT*®, *Windows Vista*™, *Internet Explorer*®, *ActiveX*® a *Active Directory*® jsou registrované ochranné známky nebo ochranné známky společnosti *Microsoft Corporation*.

Mac OS® a *Safari*™ jsou registrované ochranné známky nebo ochranné známky společnosti *Apple Computer, Inc.*

Linux® je registrovaná ochranná známka, jejímž držitelem je Linus Torvalds.

Mozilla® a *Firefox*® jsou registrované ochranné známky společnosti *Mozilla Foundation*.

Kerberos™ je ochranná známka *Massachusetts Institute of Technology* (*MIT*).

Ostatní uvedené názvy skutečných společností a produktů mohou být registrovanými ochrannými známkami nebo ochrannými známkami jejich vlastníků.

Příloha B

Použitý software open source

Produkt *Kerio WinRoute Firewall* obsahuje následující software volně šiřitelný ve formě zdrojových kódů (open source):

bindlib

Copyright © 1983, 1993 The Regents of the University of California. All rights reserved.
Portions Copyright © 1993 by Digital Equipment Corporation.

Firebird

Tento produkt obsahuje nezměněnou verzi databázového jádra *Firebird* šířeného v souladu s licencemi *IPL* a *IDPL*.
Všechna práva vyhrazena individuálním přispěvatelům — originální kód Copyright © 2000 *Inprise Corporation*.
Originální zdrojový kód je dostupný na adrese:

http://www.firebirdsql.org/

h323plus

Tento produkt obsahuje nezměněnou verzi knihovny *h323plus* šířené v souladu s *Mozilla Public License* (*MPL*).
Originální zdrojový kód je dostupný na adrese:

http://h323plus.org/

KIPF — driver

Kerio IP filter driver for Linux (síťový ovladač *WinRoute* pro Linux)
Copyright © Kerio Technologies s.r.o.
Domovská stránka: http://www.kerio.cz/
Kerio IP filter driver for Linux je šířen v souladu s licencí *GPL* verze 2.
Kompletní zdrojový kód je dostupný na adrese:

http://download.kerio.cz/dwn/libkipf.tgz

KIPF — API

Kerio IP filter driver for Linux (API knihovna síťového ovladače *WinRoute* pro Linux)
Copyright © Kerio Technologies s.r.o.
Domovská stránka: http://www.kerio.cz/
Kerio IP filter driver for Linux API library je šířena v souladu s licencí *LGPL* verze 2.
Kompletní zdrojový kód je dostupný na adrese:

http://download.kerio.cz/dwn/libkipf.tgz

KVNET — driver

Kerio Virtual Network Interface driver for Linux (ovladač virtuálního síťového rozhraní *Kerio VPN*)
Copyright © Kerio Technologies s.r.o.
Domovská stránka: http://www.kerio.cz/
Kerio Virtual Network Interface driver for Linux je šířen v souladu s licencí *GPL* verze 2.
Kompletní zdrojový kód je dostupný na adrese:

http://download.kerio.cz/dwn/libkvnet.tgz

KVNET — API

Kerio Virtual Network Interface driver for Linux API library (API knihovna ovladače virtuálního síťového rozhraní *Kerio VPN*)
Copyright © Kerio Technologies s.r.o.
Domovská stránka: http://www.kerio.cz/
Kerio Virtual Network Interface driver for Linux API library je šířena v souladu s licencí *LGPL* verze 2.
Kompletní zdrojový kód je dostupný na adrese:

http://download.kerio.cz/dwn/libkvnet.tgz

libcurl

Copyright © 1996-2008 Daniel Stenberg.

libiconv

libiconv provádí konverze různých znakových sad prostřednictvím konverze z/do Unicode. *WinRoute* obsahuje upravenou verzi této knihovny, která je šířena v souladu s licencí *LGPL* verze 3.
Copyright ©1999-2003 Free Software Foundation, Inc.
Autor: Bruno Haible
Domovská stránka: http://www.gnu.org/software/libiconv/
Kompletní zdrojový kód upravené knihovny *libiconv* je k dispozici na adrese:

http://download.kerio.cz/dwn/kwf-iconv.zip

libxml2

Copyright © 1998-2003 Daniel Veillard. All Rights Reserved.
Copyright © 2000 Bjorn Reese and Daniel Veillard.
Copyright © 2000 Gary Pennington and Daniel Veillard
Copyright © 1998 Bjorn Reese and Daniel Stenberg.

OpenSSL

Tento produkt obsahuje software vyvinutý sdružením *OpenSSL Project* pro *OpenSSL Toolkit* (http://www.openssl.org/).
Tento produkt obsahuje kryptografický kód, jehož autorem je Eric Young.
Tento produkt obsahuje software, jehož autorem je Tim Hudson.

PHP

Copyright © 1999 - 2006 The PHP Group. All rights reserved.
Tento produkt obsahuje software *PHP*, volně dostupný na adrese:

http://www.php.net/software/

php_mbstring

Copyright © 2001-2004 The PHP Group.
Copyright © 1998-2002 HappySize, Inc. All rights reserved.

Prototype

Framework (knihovna funkcí) v jazyce JavaScript.
Copyright © Sam Stephenson.
Knihovna *Prototype* je volně šiřitelná v souladu s licencí typu *MIT*.
Podrobné informace jsou uvedeny na domovská stránce knihovny *Prototype*: http://www.prototypejs.org/

ptlib

Tento produkt obsahuje nezměněnou verzi knihovny *ptlib* šířené v souladu s *Mozilla Public License* (*MPL*).
Originální zdrojový kód je dostupný na adrese:

http://h323plus.org/

zlib

Copyright © Jean-Loup Gailly and Mark Adler.

Slovníček pojmů

ActiveX

Proprietární technologie společnosti *Microsoft* určená k vytváření dynamických objektů na WWW stránkách. Tato technologie poskytuje poměrně široké možnosti, mimo jiné zápis na disk nebo spouštění příkazů na klientovi (tj. počítači, na kterém byla otevřena příslušná WWW stránka). Viry nebo červy dokáží prostřednictvím technologie *ActiveX* např. změnit telefonní číslo vytáčené linky.
Technologie *ActiveX* je podporována pouze ve WWW prohlížeči *Internet Explorer* v operačním systému *Microsoft Windows*.

Brána

Síťové zařízení nebo počítač spojující dvě různé subsítě. Pokud je přes danou bránu směrována komunikace do všech ostatních (neurčených) sítí, pak takovou bránu nazýváme výchozí branou.
Viz též *výchozí brána.*

Cluster

Skupina dvou nebo více počítačů, která tvoří jeden virtuální počítač (server). Požadavky na virtuální server jsou rozdělovány mezi jednotlivé počítače v clusteru podle definovaného algoritmu. Clustery se vytvářejí za účelem zvýšení výkonu a zvýšení spolehlivosti (při výpadku jednoho počítače v clusteru zůstává virtuální server stále funkční).

DDNS

DDNS (*Dynamic Domain Name System*) je DNS s možností automatické aktualizace záznamů.

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.

DMZ

DMZ (demilitarizovaná zóna) je označení pro vyhrazenou subsíť, ve které jsou provozovány služby přístupné z Internetu i z lokální sítě (např. veřejný WWW server firmy). Základní myšlenkou DMZ je oddělené fyzické umístění veřejně přístupných serverů, aby ani v případě jejich napadení nemohlo dojít k průniku do lokální sítě.
Bližší informace (v angličtině) lze nalézt např. v encyklopedii Wikipedia.

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*.

FTP

Protokol pro přenos souborů (*File Transfer Protocol*). Tento protokol používá dvě TCP spojení: řídicí a datové. Řídicí spojení navazuje vždy klient. Podle způsobu navazování datového spojení rozlišujeme dva režimy FTP:

- *aktivní režim* — datové spojení navazuje server na klienta (na port určený klientem). Tento režim je vhodný v případě firewallu na straně serveru, někteří klienti jej však nepodporují (např. WWW prohlížeče).
- *pasivní režim* — datové spojení navazuje rovněž klient (na port určený serverem). Tento režim je vhodný v případě firewallu na straně klienta a měl by být podporován všemi FTP klienty.

Poznámka: WinRoute obsahuje speciální podporu (inspekční modul) protokolu FTP, a proto lze na počítačích v lokální síti provozovat FTP v obou režimech bez omezení.

Greylisting

Metoda ochrany *SMTP* serveru proti nevyžádané poště (spamu). Pokud server přijme zprávu od dosud neznámého odesílatele, napoprvé ji odmítne (tzv. dočasná chyba doručení). Legitimní odesílatel se po určité době pokusí odeslání zprávy zopakovat. Při opakovaném pokusu již SMTP server zprávu přijme, začne tohoto odesílatele považovat za důvěryhodného a další zprávy od něj již nebude blokovat. Většina rozesílatelů spamu se však snaží odeslat co největší počet zpráv v co nejkratším čase a pokud možno zůstat v anonymitě. Proto po prvním odmítnutí zprávy její odeslání již neopakují a pokusí se využít jiný SMTP server.

Bližší informace (v angličtině) lze nalézt např. v encyklopedii Wikipedia.

Ident

Protokol *Ident* slouží k identifikaci uživatele, který navázal určité TCP spojení z daného (víceuživatelského) systému. Službu *Ident* využívají např. IRC servery, FTP servery a některé další služby.

Bližší informace (v angličtině) lze nalézt např. v encyklopedii Wikipedia.

IMAP

Internet Message Access Protocol je protokol elektronické pošty umožňující klientům pracovat se svými zprávami na serveru bez nutnosti stahování na lokální počítač. Uživatel se tak může připojovat k serveru z více různých počítačů a má vždy k dispozici všechny své zprávy.

Inspekční modul

Modul (podprogram) *WinRoute*, který dokáže sledovat komunikaci určitým aplikačním protokolem (např. HTTP, FTP, MMS apod.). Inspekční modul umožňuje kontrolovat správnou syntax příslušného protokolu (chyby v protokolu mohou signalizovat pokus o útok), zajistit jeho plnou funkčnost při průchodu přes firewall (např. FTP v aktivním režimu, kdy je datové spojení navazováno serverem na klienta), filtrovat komunikaci obsluhovaným protokolem (např. omezování přístupu na WWW stránky dle URL, antivirová kontrola stahovaných objektů apod.).

Není-li komunikačními pravidly stanoveno jinak, pak je každý inspekční modul automaticky aplikován na všechna spojení příslušného protokolu, která přes *WinRoute* procházejí.

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).

IPSec

IPSec (*IP Security Protocol*) je rozšíření protokolu IP umožňující zabezpečený přenos dat. Poskytuje podobné služby jako SSL/TLS, ale na síťové vrstvě. Pomocí protokolu IPSec lze vytvářet šifrované tunely mezi sítěmi (VPN) — tzv. tunelový režim, nebo šifrovat komunikaci mezi dvěma počítači — tzv. transportní režim.

Kerberos

Systém pro bezpečné ověřování uživatelů v síťovém prostředí. Byl vyvinut na univerzitě *MIT* a je standardně používán pro ověřování uživatelů v prostředí domény *Windows 2000/2003/2008*. Uživatelé se přihlašují svým heslem k centrálnímu serveru (*Key Distribution Center — KDC*) a od něho dostávají šifrované vstupenky (tickets) pro přihlášení k serverům v síti. V případě domény *Windows 2000/2003/2008* plní funkci *KDC* příslušný doménový server.

LDAP

Lightweight Directory Access Protocol je protokol pro přístup k adresářovým službám (např. *Microsoft Active Directory*). V adresářích bývají uloženy informace o uživatelských účtech a jejich právech, počítačích v síti apod.

Maska subsítě

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

NAT

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

- překlad zdrojových adres (*Source NAT, SNAT*) — v paketech jdoucích z lokální sítě do Internetu se zdrojová (privátní) IP adresa nahrazuje vnější (veřejnou) adresou 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.
Podrobný popis *NAT* (v angličtině) lze nalézt např. v encyklopedii Wikipedia.

P2P sítě

Peer-to-Peer sítě (zkr. *P2P* sítě) je označení pro celosvětové distribuované systémy, ve kterých může každý uzel sloužit zároveň jako klient i jako server. Tyto sítě slouží ke sdílení velkého objemu dat mezi uživateli (většinou soubory s nelegálním obsahem). Typickými představiteli těchto sítí jsou např. *DirectConnect* nebo *Kazaa*.

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.

Policy routing

Pokročilá technika směrování, kdy se kromě cílové IP adresy pracuje s dalšími informacemi (zdrojová IP adresa, protokol apod.).
Viz též *směrovací tabulka.*

POP3

Post Office Protocol je protokol pro přístup k elektronické poště, který umožňuje uživatelům stahovat zprávy ze serveru na lokální disk. Je vhodný zejména pro klienty, kteří nemají trvalé připojení k Internetu.

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).

PPTP

Proprietární protokol firmy *Microsoft* pro vytváření virtuálních privátních sítí.
Viz *VPN*.

Privátní IP adresy

Pro lokální sítě, které nejsou součástí Internetu (tzv. privátní sítě), jsou vyhrazeny určité rozsahy IP adres (tzv. privátní adresy). Tyto adresy se nemohou vyskytovat nikde v Internetu — tak je zajištěno, že se rozsah adres zvolený pro lokální síť nebude překrývat s adresami v Internetu.

Pro privátní sítě lze použít tyto rozsahy IP adres:

- 10.0.0.0/255.0.0.0
- 172.16.0.0/255.240.0.0
- 192.168.0.0/255.255.0.0

Proxy server

Starší, avšak stále poměrně rozšířený způsob sdílení internetového připojení. Proxy server představuje prostředníka mezi klientem a cílovým serverem.

Proxy server pracuje na aplikační úrovni a je přizpůsoben několika konkrétním aplikačním protokolům (např. HTTP, FTP, Gopher). Vyžaduje rovněž podporu v příslušné klientské aplikaci (např. WWW prohlížeči). 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.

Skript

Výkonný kód na WWW stránce, který provádí klient (WWW prohlížeč). Skripty slouží k vytváření dynamických prvků na WWW stránkách, mohou však být zneužity pro zobrazování reklam, získávání informací o uživateli apod. Moderní WWW prohlížeče podporují několik skriptovacích jazyků, mezi nejrozšířenější patří *JavaScript* a *Visual Basic Script (VBScript)*.

SMTP

Simple Mail Transfer Protocol je základní protokol, který se používá pro odesílání elektronické pošty v Internetu. Odesílatel a příjemce zprávy je určen e-mailovou adresou.

Směrovací tabulka
: Množina pravidel pro posílání paketů mezi jednotlivými rozhraními daného systému (tzv. cesty). Směrování se provádí podle cílové IP adresy paketu. V operačních systémech *Windows* lze směrovací tabulku zobrazit příkazem `route print`, v systémech typu *Unix* (*Linux*, *Mac OS X* apod.) příkazem `route`.

Směrovač
: Počítač nebo zařízení se dvěma či více síťovými rozhraními, mezi kterými předává pakety podle určitých pravidel (tzv. cest). Účelem směrovače je předávat pakety pouze do cílové sítě, resp. do sítě, kterou budou předány dalšímu směrovači na cestě k cíli. Tím brání zahlcení ostatních sítí pakety, které jsou určeny do jiné sítě.
Viz též *směrovací tabulka.*

Spam
: Nevyžádaná e-mailová zpráva, zpravidla s nabídkou určitých produktů nebo služeb.

Spojení
: Virtuální obousměrný komunikační kanál mezi dvěma počítači.
Viz též *TCP*

Spoofing
: Falšování zdrojové IP adresy v paketu. Tuto techniku používají útočníci, aby se příjemce domníval, že přijatý paket přichází z důvěryhodné IP adresy.

SSL
: Protokol *Secure Socket Layer* slouží k zabezpečení a šifrování TCP spojení. Původně byl navržen 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) — urgentní 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*.

WinRoute obsahuje proprietární implementaci VPN nazvanou *Kerio VPN*.

Výchozí brána

Síťové zařízení nebo počítač, přes který vede tzv. výchozí cesta (cesta do „zbytku Internetu“). Na adresu výchozí brány se posílají všechny pakety, jejichž cílové adresy nepatří do žádné z přímo připojených sítí ani do žádné sítě, pro kterou existuje záznam v systémové směrovací tabulce.

V systémové směrovací tabulce se výchozí brána zobrazuje jako cesta do cílové sítě *0.0.0.0* s maskou subsítě *0.0.0.0*.

Poznámka: Přestože se v operačních systémech *Windows* nastavuje výchozí brána ve vlastnostech síťového rozhraní, má globální platnost v celém operačním systému.

WINS

Služba *WINS (Windows Internet Name Service)* zajišťuje převod jmen počítačů na IP adresy v sítích *Microsoft Windows*.

Rejstřík