Kerio Control

Příručka administrátora

Kerio Technologies

Tento manuál popisuje konfiguraci a správu produktu Kerio Control ve verzi 7.4.0. Změny vyhrazeny. Uživatelské webové rozhraní a rozhraní Kerio Clientless SSL-VPN jsou popsána v samostatném manuálu *Kerio Control — Příručka uživatele*. Aplikace Kerio VPN Client pro platformy Windows a Mac OS X je popsána v samostatných manuálech *Kerio VPN Client — Příručka uživatele*.

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

Informace o registrovaných ochranných známkách a ochranných známkách jsou uvedeny v příloze A.

Produkty Kerio Control 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 Control* okamžitě sloužit pro sdílení internetového připojení a ochranu vaší lokální sítě. Podrobný postup rychlé instalace a konfigurace naleznete v samostatném manuálu *Kerio Control — Konfigurace krok za krokem*.

Nebudete-li si jisti některým nastavením *Kerio Control*, 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 s Kerio Control, resp. zařízení Kerio Control Box.

1. Nainstalujte nebo spusťte vybranou edici Kerio Control.

2. Ve WWW prohlížeči otevřete rozhraní *Kerio Control Administration*. Přímo na serveru je toto rozhraní k dispozici na adrese `http://IP_adresa_serveru:4080/` (podrobnosti viz kapitola 4).

3. Pomocí *Průvodce aktivací* (viz kapitola 5.3) aktivujte produkt s platnou licencí nebo třicetidenní zkušební verzi.

4. Pomocí *Průvodce připojením* (viz kapitola 8.1) nastavte připojení k Internetu a k lokální síti.

5. Pomocí *Průvodce komunikačními pravidly* (viz kapitola 9.1) vytvořte základní komunikační pravidla (pro lokální komunikaci, přístup do Internetu a mapování služeb).

6. Zkontrolujte nastavení modulu *DNS*. Chcete-li využívat tabulku jmen počítačů a/nebo tabulku DHCP serveru, nezapomeňte uvést lokální DNS doménu. Podrobnosti viz kapitola 11.1.

7. Nastavte mapování uživatelů z domény *Active Directory* nebo *Open Directory*, případně vytvořte nebo importujte lokální uživatelské účty a skupiny. Nastavte uživatelům požadovaná přístupová práva. Podrobnosti viz kapitola 18.

8. Zapněte systém prevence útoků (viz kapitola 10.1).

9. Povolte antivirový modul a nastavte typy objektů, které mají být kontrolovány.

10. Definujte skupiny IP adres (kapitola 17.1), časové intervaly (kapitola 17.2) a skupiny URL (kapitola 17.4), které použijete při definici pravidel (viz kapitola 17.2).

11. Zajistěte optimální využití internetového připojení nastavením pravidel pro řízení šířky pásma (kapitola 12).

12. Vytvořte pravidla pro URL (kapitola 15.2). Nastavte modul *Kerio Control Web Filter* (kapitola 15.3) a automatickou konfiguraci WWW prohlížečů (kapitola 11.4).

13. Definujte pravidla pro FTP (kapitola 15.5).

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

    - *Automatická konfigurace* — povolte automatické nastavení (výchozí nastavení ve většině operačních systémů). Nenastavujte žádné další parametry.

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

Kapitola 2

Instalace

2.1 Edice produktu

Kerio Control je k dispozici v těchto edicích:

Edice pro systém Windows
: Softwarová aplikace určená k instalaci na systém Microsoft Windows.
Může být provozována na stejném serveru s dalšími aplikacemi a službami (např. komunikačním serverem *Kerio Connect*).

Software Appliance
: *Kerio Control Software Appliance* (tzv. softwarové zařízení) je kompletní balík produktu *Kerio Control* včetně speciálního operačního systému.
Tato edice je distribuována ve formě instalačního disku a je určena pro instalaci na počítač PC bez operačního systému. *Software Appliance* nelze nainstalovat na počítač společně s jiným operačním systémem a nelze do něj ani instalovat vlastní aplikace.

Virtual Appliance
: Virtuální zařízení určené k provozování v tzv. hypervizorech. Jedná se o edici *Software Appliance*, předinstalovanou do virtuálního počítače pro příslušnou platformu.
V současnosti jsou podporovány hypervizory *VMware*, *Parallels* a *Hyper-V*.

Kerio Control Box
: Hardwarové zařízení, které stačí pouze připojit do sítě. Je dostupné ve dvou variantách, které se liší výkonem a počtem síťových portů.

Edice *Software Appliance*, *VMware Virtual Appliance*, *Virtual Appliance for Parallels* a *Virtual Appliance for Hyper-V* budou pro jednoduchost dále označovány souhrnným názvem *Appliance*, zařízení *Kerio Control Box* bude dále označováno zkráceným názvem *Box*.

2.2 Systémové požadavky

Aktuální systémové požadavky softwarových edic a technickou specifikaci hardwarového zařízení *Kerio Control Box* naleznete na stránce:

http://www.kerio.cz/cz/control/technical-specifications

2.3 Windows: Konfliktní software

Kerio Control 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 *Kerio Control* 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 *Kerio Control*.

Kolize nízkoúrovňových ovladačů

Kerio Control 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 *Kerio Control* 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). *Kerio Control* 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 *Kerio Control* může být používán společně se službou *RRAS*.
- Síťové firewally — např. *Microsoft ISA Server / Forefront TMG*.
- Osobní firewally — např. *Zone Alarm*, *ESET Smart Security* apod.
- Software pro vytváření virtuálních privátních sítí (VPN) — např. firem *CheckPoint*, *Cisco Systems* 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 v *Kerio Control* (podrobnosti viz kapitola 25). V opačném případě doporučujeme otestovat konkrétní VPN server či VPN klienta se zkušební verzí *Kerio Control* a případně kontaktovat technickou podporu firmy *Kerio Technologies*.
  Poznámka:
  Implementace VPN obsažená v operačním systému *Windows* (založená na protokolu PPTP) je v *Kerio Control* podporována.

Kolize portů

Na počítači, kde je *Kerio Control* nainstalován, nemohou být provozovány aplikace, které využívají tytéž porty (nebo je třeba konfiguraci portů změnit).
Pokud jsou zapnuty všechny služby, které *Kerio Control* nabízí, pak *Kerio Control* 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 20.2).
- `4080/TCP` — nezabezpečené WWW rozhraní firewallu (viz kapitola 14). Tuto službu nelze vypnout.
- `4081/TCP` — zabezpečená (SSL) verze WWW rozhraní firewallu (viz kapitola 14).

Tuto službu nelze vypnout.

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

- `443/TCP` — server rozhraní *SSL-VPN* (pouze v *Kerio Control* na systému *Windows* — viz kapitola 26),
- `3128/TCP` — HTTP proxy server (viz kapitola 11.5),
- `4090/TCP+UDP` — proprietární VPN server (podrobnosti viz kapitola 25).

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. *Kerio Control* rovněž poskytuje tuto funkci, a proto zde dochází ke kolizím. Z tohoto důvodu doporučujeme na počítač s *Kerio Control* instalovat vždy serverovou verzi zvoleného antivirového programu. Serverovou verzi antiviru lze zároveň využít pro kontrolu síťové komunikace v *Kerio Control*, případně jako doplňkovou kontrolu k integrovanému antivirovému modulu *Sophos* (podrobnosti viz kapitola 16).

Má-li antivirový program tzv. rezidentní štít (automatická kontrola všech čtených a zapisovaných souborů), pak je třeba z kontroly vyloučit podadresáře `cache` (HTTP cache *Kerio Control* — viz kapitola 11.4) a `tmp` (používá se pro antivirovou kontrolu). Pokud *Kerio Control* prování antivirovou kontrolu objektů stahovaných protokoly HTTP a FTP (viz kapitola 16.3), 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 *Sophos* nevykazuje žádnou interakci s antivirovým programem nainstalovaným na počítači s *Kerio Control* (za předpokladu, že jsou splněny výše uvedené podmínky).

2.4 Windows: Instalace

Instalační balíky

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

Kroky před spuštěním instalace

Kerio Control 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, Wi-Fi apod.) a rozhraní připojené k Internetu. Internetovým rozhraním může být buď síťový adaptér (Ethernet, Wi-Fi atd.) nebo modem (analogový, ISDN apod.).

Před zahájením instalace *Kerio Control* doporučujeme prověřit následující:

- Správné nastavení systémového času (nutné pro kontrolu aktualizací operačního systému, antivirového modulu 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`).

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

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

Postup instalace a počáteční konfigurace

Po spuštění instalačního programu (např. `kerio-control-1.2.3-4567-win32.exe`) lze vybrat jazyk instalačního programu. Výběr jazyka ovlivňuje pouze samotnou instalaci, jazyk uživatelského rozhraní lze pak nastavit nezávisle pro jednotlivé komponenty *Kerio Control*.

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

- *Kerio Control Engine* — vlastní výkonné jádro aplikace.
- *Podpora VPN* — proprietární VPN řešení firmy *Kerio Technologies* (*Kerio VPN*).

Podrobný popis komponent *Kerio Control* naleznete v kapitole 3. Proprietární VPN řešení je detailně popsáno v kapitole 25.

Poznámka:
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 *Kerio Control* přes stávající (upgrade) je tedy třeba označit všechny komponenty, které mají zůstat zachovány.

Vzdálený přístup

Bezprostředně po prvním spuštění *Kerio Control Engine* dojde k blokování veškeré síťové komunikace (požadovaná komunikace pak musí být povolena vytvořením pravidel — viz kapitola 9). Je-li *Kerio Control* instalován vzdáleně (např. pomocí terminálového přístupu), pak se v tomto okamžiku přeruší také komunikace se vzdáleným klientem (a konfigurace *Kerio Control* musí být provedena lokálně).

Pro umožnění vzdálené instalace a správy lze v instalačním průvodci povolit komunikaci mezi *Kerio Control* a vzdáleným počítačem.

Poznámka:

1. Pokud *Kerio Control* instalujete lokálně, pak tento krok přeskočte. Povolení plného přístupu ze vzdáleného počítače může představovat bezpečnostní hrozbu.
2. Po nastavení *Kerio Control* průvodcem komunikačními pravidly (viz kapitola 9.1) se pravidlo pro povolení vzdáleného přístupu zruší.

Kolizní programy a systémové služby

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

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

   Tyto komponenty zajišťují podobné nízkoúrovňové funkce jako *Kerio Control*. Pokud by byly spuštěny společně s *Kerio Control*, nefungovala by síťová komunikace správně a *Kerio Control* 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 *Kerio Control 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*. Tyto služby však vykazují kolize s podporou protokolu *UPnP* v *Kerio Control* (viz kapitola 20.2).

[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*.

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

Ve výchozím nastavení instalační program *Kerio Control* 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 *Kerio Control* fungovat správně. Uvedenou volbu při instalaci lze chápat spíše jako varování, že tato služba je spuštěna a musí být zastavena a zakázána.

- Pokud chcete využít podporu protokolu *UPnP* v *Kerio Control* (viz kapitola 20.2), pak je nutné zakázat také služby *Hostitel zařízení UPnP* (*UPnP Device Host*) a *Služba rozpoznávání pomocí protokolu SSDP* (*SSDP Discovery*).

- Nechceme-li využívat podporu *UPnP* v *Kerio Control*, není nutné uvedené služby zakazovat.

Poznámka:

1. *Kerio Control* 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 *Kerio Control* nainstalován.
2. V operačních systémech *Windows XP Service Pack 2*, *Windows Server 2003*, *Windows Vista*, *Windows Server 2008* a *Windows 7* se *Kerio Control* 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.

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 *Kerio Control* 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 *Kerio Control* výše popsaným způsobem zabezpečit. Z tohoto důvodu doporučujeme instalovat *Kerio Control* výhradně na disk se souborovým systémem *NTFS*.

Spuštění průvodce aktivací produktu

Před dokončením instalace se automaticky spustí *Kerio Control Engine*, tj. vlastní výkonné jádro programu (běží jako systémová služba) a také *Kerio Control Engine Monitor*.

Po ukončení instalačního průvodce se automaticky otevře rozhraní *Kerio Control Administration* ve výchozím WWW prohlížeči. V tomto rozhraní se nejprve spustí průvodce aktivací produktu (viz kapitola 5.3).

2.5 Windows: Upgrade a deinstalace

Upgrade

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

Instalační program sám ukončí komponenty *Kerio Control Engine* a *Kerio Control Engine Monitor*.

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:
Aktualizaci na verzi 7.4.x lze provést z verze 7.1.0 a novějších. V případě aktualizace ze starší verze je nutné nejprve nainstalovat verzi 7.1.0 (ke stažení v softwarovém archivu Kerio Technologies).

Automatická kontrola nových verzí

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

Podrobné informace naleznete v kapitole 19.2.

Deinstalace

Pro deinstalaci je vhodné ukončit všechny komponenty *Kerio Control*. Program lze deinstalovat průvodcem *Přidat nebo odebrat programy* v *Ovládacích panelech*. Při deinstalaci mohou být volitelně smazány také všechny soubory v instalačním adresáři *Kerio Control*

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

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

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

Při deinstalaci instalační program *Kerio Control* 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*).

2.6 Appliance Edition: Instalace

Instalace *Software Appliance* probíhá v několika jednoduchých krocích:

Spuštění instalace

Software Appliance

Edici Software Appliance můžete nainstalovat těmito způsoby:

- Vypálit ISO obraz instalačního CD 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.
- Vytvořit z ISO obrazu bootovatelný USB flash disk. Podrobný postup naleznete v kapitole 27.1.

Poznámka:
Kerio Control 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

Podle typu produktu *VMware* použijte odpovídající instalační balík:

- V případě produktů *VMware Server, Workstation, Player* a *Fusion* stáhněte distribuční balík ve formátu *VMX* (`*.zip`), rozbalte jej a otevřete soubor s příponou `.vmx`.
- Do *VMware ESX/ESXi* můžete přímo importovat virtuální zařízení ze zadané URL adresy *OVF* souboru — např.:

  ```
  http://download.kerio.com/cz/dwn/control/
  kerio-control-appliance-1.2.3-4567-linux.ovf
  ```

  VMware ESX/ESXi si automaticky stáhne daný konfigurační *OVF* soubor a odpovídající obraz disku (soubor s příponou `.vmdk`).

V případě importu virtuálního zařízení ve formátu *OVF* je potřeba mít na paměti následující specifické vlastnosti:

- V importovaném virtuálním zařízení je vypnuta synchronizace času mezi hostitelským počítačem a virtuálním zařízením. Produkt *Kerio Control* však disponuje vlastním mechanismem pro synchronizaci času s časovými servery

v Internetu, a proto není nutné synchronizaci s hostitelským počítačem explicitně povolovat.

- Akce pro vypnutí, resp. restart virtuálního počítače budou po importu nastaveny na výchozí hodnoty, což může být „tvrdé“ vypnutí a „tvrdý“ reset. To však může způsobit ztrátu dat ve virtuálním zařízení. *Kerio Control VMware Virtual Appliance* podporuje tzv. *Soft Power Operations*, které umožňují regulérně vypnout nebo restartovat hostovaný operační systém. Proto je doporučeno jako akce pro vypnutí a restart nastavit vypnutí, resp. restart hostovaného operačního systému.

Virtual Appliance for Parallels

Rozbalte distribuční balík do požadovaného cílového umístění a otevřete konfigurační soubor virtuálního zařízení (`config.pvs`) v aplikaci Parallels. Žádná speciální nastavení nejsou potřeba.

Virtual Appliance for Hyper-V

Stáhněte distribuční balík ve formátu *Zip* (`*.zip`) a rozbalte jej do požadovaného cílového umístění.

Vytvořte nové virtuální zařízení. V průvodci zvolíme možnost „použít existující virtuální disk“ a použijte virtuální disk z distribučního balíku.

Volba jazyka

Zvolený jazyk bude použit nejen pro instalaci *Kerio Control*, ale také pro konzoli firewallu (viz kapitola 3.2).

Výběr cílového pevného disku (Software Appliance)

Pokud instalační program Software Appliance detekuje v počítači více pevných disků, pak je potřeba zvolit disk, na který má být *Kerio Control* nainstalován. Obsah vybraného disku bude před vlastní instalací *Kerio Control* 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.

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

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 budete 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 — vyberte

některé rozhraní, dokončete instalaci a zkuste se připojit ke správě. Pokud se připojení nepodaří, změňte nastavení jednotlivých rozhraní volbou *Konfigurace sítě* v hlavní nabídce konzole firewallu (viz kapitola 3.2).

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 *Kerio Control Software Appliance* do jiného typu virtuálního počítače. Tento problém doporučujeme konzultovat s technickou podporou společnosti *Kerio Technologies*.

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

Poznámka:
Instalační program umožňuje nastavit na rozhraních nastavit pouze parametry protokolu IPv4. Protokol IPv6 je možné nastavit pouze ve webovém rozhraní Kerio Control Administration.

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).
- *Kerio Control* bude pravděpodobně ve většině případů sám sloužit jako DHCP server pro počítače (pracovní stanice) v lokální síti.

Dokončení instalace

Po nastavení všech uvedených parametrů se spustí služba (daemon) *Kerio Control Engine*. Na konzoli firewallu bude po celou dobu jeho běhu zobrazena informace o možnostech vzdálené správy a změny některých základních nastavení — viz kapitola 3.2.

2.7 Appliance Edition: Upgrade

Upgrade (aktualizaci) *Kerio Control* lze provést dvěma způsoby:

- Spouštěním systému z instalačního CD (resp. USB flash disku nebo 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 2.6.
- Prostřednictvím kontroly nových verzí v rozhraní *Kerio Control Administration*. Podrobnosti naleznete v kapitole 19.2.

Upozornění:
Aktualizaci na verzi 7.4.x lze provést z verze 7.1.0 a novějších. V případě aktualizace ze starší verze je nutné nejprve nainstalovat verzi 7.1.0 (ke stažení v softwarovém archivu Kerio Technologies).

Kapitola 3

Komponenty Kerio Control

Kerio Control sestává z těchto součástí:

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

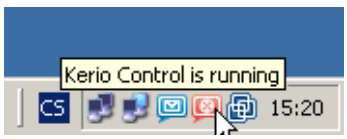
Kerio Control Engine Monitor (pouze Windows)
: Slouží k monitorování a změně stavu *Engine* (zastaven / spuštěn), nastavení spouštěcích preferencí (tj. zda se má *Engine* a/nebo *Monitor* sám spouštět automaticky při startu systému) a snadnému spuštění administrační konzole. Podrobnosti naleznete v kapitole 3.1.
Poznámka:
Kerio Control Engine je zcela nezávislý na aplikaci *Kerio Control Engine Monitor*. *Engine* tedy může být spuštěn, i když se na liště právě nezobrazuje ikona.

Konzole firewallu (pouze edice Appliance a Box)
: Konzole firewallu je jednoduché rozhraní, které je trvale spuštěné na počítači s *Kerio Control*. Umožňuje nastavení základních parametrů operačního systému a firewallu, případně obnovení přístupu ke správě, pokud došlo k jejímu zablokování.

Poznámka: Od verze *7.1.0* již není k dispozici samostatný program pro správu (*Kerio Administration Console*).

3.1 Kerio Control Engine Monitor (Windows)

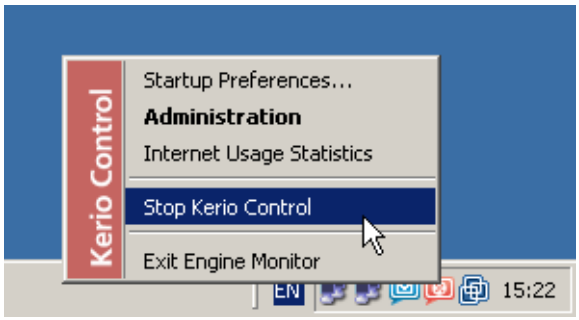
Kerio Control Engine Monitor je samostatný program, který slouží k ovládání a sledování stavu *Kerio Control Engine*. Tato komponenta se zobrazuje jako ikona na nástrojové liště.



Obrázek 3.1 Ikona programu Kerio Control Engine Monitor v oznamovací oblasti nástrojové lišty

Je-li *Kerio Control Engine* zastaven, objeví se přes ikonu červený kruh s bílým křížkem. Spouštění či zastavování *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 otevřít rozhraní *Kerio Control Administration* ve výchozím WWW prohlížeči (viz dále). Po kliknutí pravým tlačítkem se zobrazí menu s následujícími funkcemi:



Obrázek 3.2 Menu programu Kerio Control Engine Monitor

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

Administration
: Otevření rozhraní *Kerio Control Administration* ve výchozím WWW prohlížeči (odpovídá dvojitému kliknutí levým tlačítkem myši na ikonu *Engine Monitoru*).

Internet Usage Statistics
: Otevření *Statistik využívání Internetu* ve výchozím WWW prohlížeči. Podrobnosti viz kapitola 23.

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

Exit Engine Monitor
: Ukončení programu *Engine Monitor*. Tato volba nezastavuje *Kerio Control Engine*, na což je uživatel upozorněn varovným hlášením.

Poznámka:

1. Pokud má licence *Kerio Control* omezenou platnost (např. 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. *Kerio Control Engine Monitor* je k dispozici pouze v anglickém jazyce.

3.2 Konzole firewallu (edice Appliance a Box)

Konzole firewallu je speciální aplikace, která je spuštěna na terminálu počítače s *Kerio Control* v edici *Appliance* po celou dobu jeho běhu. V případě zařízení *Kerio Control Box* je možné se ke konzoli připojit prostřednictvím sériového portu.

Ve výchozím stavu zobrazuje konzole pouze informace o URL, resp. IP adrese, kam se lze připojit ke správě firewallu prostřednictvím WWW prohlížeče (rozhraní *Kerio Control Administration*). Po zadání hesla uživatele *Admin* (hlavního správce firewallu) tato konzole umožňuje změnit některá základní nastavení, obnovit výchozí nastavení po instalaci a vypnout nebo restartovat počítač. 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. Konzole umožňuje pouze konfiguraci parametrů protokolu IPv4 (k nastavení parametrů IPv6 je potřeba použít webové administrační rozhraní).

Na každém rozhraní lze nastavit automatickou konfiguraci protokolem DHCP nebo ručně zadat IP adresu, masku subsítě a výchozí bránu.

Konzole rovněž umožňuje definovat nové virtuální sítě (VLAN) na vybraném rozhraní typu Ethernet. Každá VLAN se chová jako samostatné rozhraní, kterému lze nastavit parametry IPv4 dle potřeby.

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 9) prostřednictvím WWW rozhraní *Kerio Control Administration* může dojít k nechtěnému zablokování přístupu ke vzdálené správě.

Pokud jste si jisti, že síťová rozhraní firewallu jsou nastavena správně, ale přesto se nelze připojit ke vzdálené správě, můžete volbou *Vzdálená správa* změnit komunikační pravidla firewallu tak, aby neblokovala přístup ke vzdálené správě přes žádné síťové rozhraní.

Po změně komunikačních pravidel bude automaticky restartována služba *Kerio Control Engine*.

„Odblokování“ vzdálené správy v praxi znamená, že na začátek tabulky komunikačních pravidel bude přidáno pravidlo povolující přístup z libovolného počítače ke službě *Kerio Control WebAdmin* (zabezpečené WWW rozhraní firewallu).

Vypnutí / restart firewallu

V případě, že potřebujete firewall vypnout nebo restartovat, tyto volby zajistí bezpečné ukončení služby *Kerio Control 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 2.6).

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 4

Správa Kerio Control

Aplikace *Kerio Control* má webové rozhraní *Kerio Control Administration* (tzv. *administrační rozhraní*), které umožňuje vzdálenou i lokální správu firewallu prostřednictvím běžného WWW prohlížeče.

4.1 Rozhraní Kerio Control Administration

Rozhraní *Kerio Control Administration* je dostupné na adrese:

`https://server:4081/admin`

(`server` má význam jména nebo IP adresy firewallu a `4081` je port jeho WWW rozhraní). Při použití protokolu *HTTPS* je komunikace mezi klientem a *Kerio Control Engine* šifrována, což zabraňuje jejímu odposlechu a zneužití. Nezabezpečenou verzi rozhraní *Administration* (protokol *HTTP*, port `4080`) doporučujeme používat pouze pro lokální správu *Kerio Control* (tj. správu z počítače, na kterém je nainstalován).

Po úspěšném přihlášení do WWW rozhraní *Administration* se zobrazí hlavní okno, které je rozděleno na dvě části:

- Levý sloupec obsahuje seznam sekcí administračního rozhraní v podobě stromu. Pro větší přehlednost lze jednotlivé části stromu skrývat a rozbalovat (bezprostředně po přihlášení je strom kompletně rozbalený).
- Pravá část okna zobrazuje obsah sekce zvolené v levém sloupci.

Ve většině případů se změny konfigurace v jednotlivých sekcích provádějí pouze na straně klienta (tj. ve WWW prohlížeči), a teprve po stisknutí tlačítka *Použít* se tyto změny aplikují a uloží do konfiguračního souboru. Díky tomu je možné tlačítkem *Storno* kdykoliv obnovit původní stav.

Jednotlivé sekce webového administračního rozhraní jsou popsány v následujících kapitolách tohoto manuálu.

Poznámka:

1. WWW rozhraní *Kerio Control Administration* je lokalizováno celkem do 15 jazyků. V rozhraní *Administration* lze zvolit jazyk pomocí ikony vlajky v pravém horním rohu okna, případně může být nastaven automaticky podle preferovaného jazyka ve WWW prohlížeči.
2. Při prvním přihlášení do rozhraní *Kerio Control Administration* po instalaci *Kerio Control* se nejprve automaticky spustí průvodce aktivací, který umožňuje zaregistrovat

zakoupenou licenci nebo spustit třicetidenní zkušební verzi a nastavit heslo pro přístup ke správě. Podrobný popis tohoto průvodce naleznete v kapitole 9.1.

4.2 Konfigurační asistent

Konfigurační asistent slouží ke snadné a rychlé konfiguraci základních parametrů *Kerio Control*. Ve výchozím nastavení se zobrazuje automaticky po přihlášení do administračního rozhraní. Pokud je jeho automatické zobrazování vypnuto, stačí kliknout na odkaz *Spustit konfiguračního asistenta*.

Konfigurační asistent nabízí tyto možnosti:

Nastavit internetové připojení a lokální síť
: Průvodce základním nastavením *Kerio Control*. Po dokončení tohoto průvodce bude funkční internetové připojení (protokol IPv4) a přístup do Internetu z počítačů v lokální síti. Průvodce zajistí správné nastavení DHCP serveru a modulu *DNS forwarder*.
Podrobný popis průvodce naleznete v kapitole 8.1.

Definovat komunikační pravidla
: Nastavení základních komunikačních pravidel firewallu. Základními pravidly se myslí povolení přístupu z lokální sítě do Internetu prostřednictvím překladu IP adres (NAT) a zpřístupnění vybraných služeb na lokálních serverech z Internetu.
Tento nástroj je určen především pro počáteční konfiguraci komunikačních pravidel. Při pozdějším použití dojde k přepsání stávajících komunikačních pravidel.
Bližší informace naleznete v kapitole 9.1.

Exportovat vaši konfiguraci
: Uložení stávající konfigurace *Kerio Control* do balíku ve formátu *.tgz* (archiv *tar* komprimovaný *gzip*).
Exportovanou konfiguraci lze použít jako zálohu pro obnovení firewallu po reinstalaci, případně pro přenos stejné konfigurace na jiný počítač. Konfigurace *Kerio Control* je přenositelná mezi jednotlivými platformami.

Import konfigurace
: Načtení a použití zálohované konfigurace firewallu. Při importu konfigurace se zohledňují rozdíly v síťových rozhraních (přidané nebo odebrané rozhraní, jiné názvy rozhraní atd.).
Podrobné informace o exportu a importu konfigurace naleznete v kapitole 27.2

Instalovat licenční klíč
: Instalace licenčního klíče (`license.key`) exportovaného nebo zálohovaného z dřívější instalace.

Registrace zakoupeného produktu, Registrace zkušební verze
: Viz kapitola 5

Poznámka:
Použití konfiguračního asistenta a jednotlivých průvodců není nutné. Zkušení správci mohou *Kerio Control* nakonfigurovat podle svých potřeb i bez použití těchto nástrojů.

4.3 Ochrana proti zablokování správy

Při změnách v konfiguraci *Kerio Control* (nastavení síťových rozhraní, komunikačních pravidel, filtru MAC adres a dalších bezpečnostních funkcí) může poměrně snadno dojít k přerušení síťového spojení mezi serverem *Kerio Control* a počítačem, ze kterého je prováděna správa (edice *Appliance* a *Box* lze spravovat pouze vzdáleně z jiného počítače).

Proto po změnách v konfiguraci, které mohou mít vliv na spojení mezi rozhraním *Kerio Control Administration* a serverem *Kerio Control*, bude automaticky provedena kontrola, zda je spojení stále funkční. Pokud dojde k přerušení spojení, rozhraní *Kerio Control Administration* se jej pokusí obnovit.

V některých případech není možné spojení automaticky obnovit — typickým příkladem je změna IP adresy rozhraní, přes které je *Kerio Control* spravován. Pak je potřeba se připojit k administračnímu rozhraní na nové IP adrese a znovu se přihlásit (k tomu může být potřeba také změna konfigurace TCP/IP na klientském počítači, případně obnovení konfigurace z DHCP serveru atd.).

Pokud se nepodaří obnovit spojení během 10 minut (případně se správci nepodaří se během této doby znovu přihlásit), server vyhodnotí, že došlo k zablokování správy, zruší poslední konfigurační změny a vrátí tak konfiguraci do předchozího stavu.

Kapitola 5

Licence a registrace produktu

Používání produktu *Kerio Control* je vázáno na licenci. Technicky se produkt chová takto:

- Bezprostředně po instalaci produkt funguje jako zkušební verze, časově omezená na dobu 30 dnů od okamžiku instalace. Produkt je plně funkční s výjimkou modulu *Kerio Control Web Filter* a aktualizací integrovaného antiviru a pravidel systému prevence útoků.

- Zkušební verzi lze bezplatně zaregistrovat. Registrací zkušební verze získává uživatel nárok na technickou podporu během zkušebního období. Navíc může také testovat modul *Kerio Control Web Filter* a bude automaticky aktualizován integrovaný antivirus a pravidla systému prevence útoků. Registrace neprodlužuje zkušební období.

- Po zakoupení licence je potřeba produkt zaregistrovat s příslušným licenčním číslem. Po úspěšné registraci bude produkt funkční po neomezenou dobu v rozsahu dle příslušné licence (podrobnosti viz kapitola 5.1).

Rozdíl mezi zkušební verzí a plnou verzí *Kerio Control* je pouze v tom, zda je zaregistrována s platnou licencí či nikoliv. Každý zákazník má tak možnost si produkt nainstalovat a během zkušební lhůty otestovat v konkrétních podmínkách. Pokud si jej zakoupí, stačí pouze zaregistrovat nainstalovanou verzi se zakoupeným licenčním číslem. Není tedy třeba *Kerio Control* znovu instalovat a nastavovat.

V případě, že třicetidenní zkušební lhůta již vypršela, funkčnost *Kerio Control* bude omezena. Po registraci s platným licenčním číslem (získaným při zakoupení produktu) bude *Kerio Control* opět plně funkční.

Licence produktu zároveň určuje počet uživatelů, kteří jej mohou využívat. Základní produktu licence je pro 5 uživatelů. Počet uživatelů lze kdykoliv rozšířit zakoupením tzv. add-on licence. Podrobnosti o stanovení správného počtu uživatelů viz kapitola 5.2.

5.1 Licence, volitelné komponenty a Software Maintenance

Produkt *Kerio Control* má volitelné komponenty: antivirový modul *Sophos* (viz kapitola 16) a modul pro hodnocení obsahu WWW stránek *Kerio Control Web Filter* (viz kapitola 15.3). Tyto komponenty jsou licencovány odděleně.

Software Maintenance

Software Maintenance je nárok na aktualizaci produktu po danou dobu. Pokud Software Maintenance vyprší, produkt je možné nadále používat, ale nelze již instalovat nové verze vydané po datu vypršení. Nárok na aktualizaci produktu lze obnovit zakoupením Software Maintenance na další období.

Licenční číslo

Od verze 7.4.0 se v Kerio Control používá pouze jedno licenční číslo, které obdržíte při zakoupení produktu. Při zakoupení volitelných komponent, zvýšení počtu uživatelů nebo prodloužení Software Maintenance se licence během 24 hodin automaticky aktualizuje.

Poznámka:

1. Registrací produktu *Kerio Control* dojde k vytvoření tzv. licenčního klíče (soubor `license.key` — viz kapitola 27.2). V případě ztráty licenčního klíče (např. z důvodu havárie disku, nechtěným smazáním apod.), stačí produkt jednoduše znovu zaregistrovat s licenčním číslem obdrženým při jeho zakoupení. Stejným způsobem lze postupovat při změně platformy firewallu (*Windows* / *Appliance* / *Kerio Control Box*) — licenční klíč je nepřenositelný mezi platformami. Při ztrátě licenčního čísla je nutné kontaktovat obchodní oddělení společnosti *Kerio Technologies*.
2. Aktuální informace o licenci a Software Maintenance naleznete na WWW stránkách firmy Kerio Technologies (http://www.kerio.cz/cz/control/).

5.2 Stanovení potřebného počtu uživatelů

Produkt *Kerio Control* je licencován jako server, který v základní licenci obsahuje účet *Admin* a 5 uživatelských účtů. Uživatele lze přidávat v balíčcích po 5.

Uživatel je definován jako osoba, který se může přihlásit ke *Kerio Control* a jeho službám. Každý uživatel se přitom může připojit až z pěti různých zařízení reprezentovaných IP adresami, včetně VPN klientů.

Pokud se jeden uživatel chce připojit z více než pěti zařízení současně, pak je potřeba licence pro dalšího uživatele. Produkt sice v minulost neomezoval počet přihlášení uživatelů, zato však považoval každou IP adresu přistupující k serveru za jednoho uživatele, takže někteří uživatele mohli vyčerpat dostupné licence již připojením ze dvou zařízení současně.

Upozornění:
Kerio Control neomezuje počet definovaných uživatelských účtů (viz kapitola 18). Při dosažení maximálního povoleného počtu současně přihlášených uživatelů však firewall nepovolí přihlášení dalšího uživatele.

5.3 Průvodce aktivací produktu

Při prvním přihlášení do rozhraní *Kerio Control Administration* bezprostředně po instalaci se automaticky spustí průvodce aktivací produktu. Tento průvodce umožňuje zaregistrovat produkt se zakoupenou licencí nebo aktivovat třicetidenní zkušební verzi a nastavit některé základní parametry *Kerio Control*.

Volba jazyka

První krok umožňuje volbu jazyka. Vybraný jazyk bude použit v průvodci aktivací a bude také přednastaven po prvním přihlášení do administračního rozhraní. Po přihlášení lze pak jazyk měnit dle potřeby.

Internetové připojení

V dalším kroku průvodce zkontroluje, zda je k dispozici připojení k Internetu a je možné registrovat produkt online.

V edicích *Appliance* a *Box*, pokud není detekováno internetové připojení, průvodce umožní změnit nastavení síťových rozhraní. Zvolte rozhraní připojené k Internetu, způsob konfigurace (DHCP, statická konfigurace nebo PPPoE) a zadejte požadované parametry. Tento postup lze opakovat, dokud se nepodaří navázat funkční připojení k Internetu.

Na systému *Windows* je nutné nastavit parametry internetového připojení přímo ve vlastnostech příslušného síťového adaptéru.

Alternativně je možné zvolit registraci offline a nastavit internetové připojení později.

Nastavení časové zóny, data a času (edice Appliance a Box)

Pro registraci a celou řadu dalších funkcí *Kerio Control* (ověřování uživatelů, záznamy, statistiky atd.) je nezbytné správné nastavení data, času a časové zóny na firewallu.

Zvolte vaši časovou zónu a zkontrolujte, případně upravte nastavení data a času. Doporučujeme povolit synchronizaci času s časovým serverem (používají se NTP servery společnosti *Kerio Technologies*).

Aktivace online

Aktivace online umožňuje zaregistrovat sériové číslo zakoupeného produktu nebo třicetidenní zkušební verzi.

Registrace zakoupené licence

K registraci si připravte licenční číslo zakoupeného produktu.

- Zadejte licenční číslo a opište bezpečnostní kód z obrázku (ochrana proti zneužití registračního serveru).
- V následujícím kroku můžete upravit vaše registrační údaje.
- Po úspěšné registraci bude automaticky vytvořen licenční klíč a produkt bude aktivován s platnou licencí.

Registrace zkušební verze

Chcete-li testovat třicetidenní zkušební verzi produktu, můžete si ji také zaregistrovat. Tato registrace je nepovinná a nezávazná.

Registrace zkušební verze umožňuje testovat také funkce, které jsou v neregistrované verzi nedostupné (modul *Kerio Control Web Filter*, aktualizace integrovaného antiviru a systému prevence útoků). Dále získáte nárok na bezplatnou technickou podporu po dobu zkušebního období.

Registrace zkušební verze neprodlužuje zkušební období.

Aktivace offline

Pro aktivaci offline je potřeba soubor s licenčním klíčem pro příslušnou platformu (soubor má obvykle název `license.key`). Tento soubor můžete mít zálohovaný z předchozí instalace *Kerio Control*.

Nemáte-li k dispozici soubor s licenčním klíčem (nebo přecházíte na jinou platformu), pak je možné zaregistrovat licenci na WWW stránkách společnosti *Kerio Technologies* (http://www.kerio.cz/, volba *Podpora* → *Zaregistrovat licenci* v hlavním menu).

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. Po úspěšné registraci licence si můžete stáhnout vygenerovaný licenční klíč a ten použít pro offline aktivaci produktu.

Neregistrovaná zkušební verze

V případě, že z nějakého důvodu není možné registraci dokončit (např. v danou nemáte k dispozici internetové připojení ani soubor s licenčním klíčem), pak lze odkazem *Přeskočit registraci* aktivovat neregistrovanou třicetidenní zkušební verzi. Produkt je pak možné zaregistrovat později pomocí odkazů na úvodní stránce administračního rozhraní.

Dobrovolné odesílání statistik používání produktu

Při vývoji produktu Kerio Control jsou pro nás užitečné informace o tom, jakým způsobem je produkt využíván. Odesíláním dobrovolných statistik můžete přispět k vylepšení produktu.

Statistiky neobsahují žádná důvěrná data (hesla, e-mailové adresy apod.) a jejich zasílání lze kdykoliv vypnout v sekci *Konfigurace* → *Další volby* → *Aktualizace* (viz kapitola 19.2).

Heslo uživatele Admin

V posledním kroku průvodce aktivací je nutné zadat heslo uživatele *Admin* — hlavního správce firewallu. Uživatelské jméno *Admin* s tímto heslem pak slouží:

- Pro přihlášení správě firewallu prostřednictvím webového administračního rozhraní (viz kapitola 4),
- V případě edic *Appliance* a *Box* také pro přihlášení konzole firewallu (viz kapitola 3.2).

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

5.4 Vypršení licence nebo práva na aktualizaci

Kerio Control automaticky upozorňuje správce na blížící se datum skončení platnosti licence a/nebo skončení práva na aktualizaci (Software Maintenance) základního produktu, integrovaného antiviru *Sophos* nebo modulu *Kerio Control Web Filter*. Hlavním účelem těchto upozornění je včas informovat správce tom, že je třeba prodloužit Software Maintenance nebo obnovit příslušnou licenci.

Tato upozornění mají následující podoby:

- Upozornění bublinovou zprávou (tyto zprávy zobrazuje komponenta *Kerio Control Engine Monitor* — pouze v operačních systémech *Windows*),
- Upozornění na vypršení licence a/nebo Software Maintenance informačním oknem po přihlášení do rozhraní *Kerio Control Administration*.
- Upozornění na skončení funkčnosti produktu ve WWW rozhraní firewallu při přístupu na WWW stránku v Internetu.

Poznámka:
Správce *Kerio Control* může rovněž nastavit zasílání výstrahy o vypršení licence nebo Software Maintenance formou e-mailu nebo krátké textové zprávy na mobilní telefon (viz kapitola 21.5).

Upozornění bublinovými zprávami (Windows)

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

Tato informace se zobrazuje až do chvíle, kdy přestane být *Kerio Control* nebo některá z jeho komponent funkční, případně kdy vyprší Software Maintenance. Informace se rovněž přestane zobrazovat bezprostředně po prodloužení Software Maintenance nebo licence příslušné komponenty.

Upozornění v administračním rozhraní

Počínaje 30. dnem před vypršením licence nebo Software Maintenance se po každém přihlášení ke správě zobrazí varování o zbývajícím počtu dnů do vypršení, případně že licence nebo Software Maintenance již vypršela. Součástí tohoto upozornění je odkaz na WWW stránky společnosti *Kerio Technologies*, kde lze získat bližší informace a zakoupit novou licenci nebo Software Maintenance na další období.

Upozornění se přestane zobrazovat po prodloužení Software Maintenance.

Upozornění ve WWW rozhraní

Toto upozornění se zobrazuje v případě časově omezených licencí (např. NFR licence) nebo časově omezených verzí (Beta a RC verze). Počínaje 7. dnem před datem skončení funkčnosti *Kerio Control* při přístupu libovolného uživatele na WWW stránku v Internetu dojde k přesměrování prohlížeče na speciální stránku WWW rozhraní firewallu. Tato stránka informuje uživatele o počtu dnů zbývajících do skončení plné funkčnosti produktu.

Poznámka:
Funkčnost finálních verzí s platnou „standardní“ licencí není časově omezena.

Kapitola 6

Podpora protokolu IPv6

Kerio Control obsahuje základní podporu protokolu IP verze 6 (IPv6). Tato podpora zahrnuje:

- Nastavení parametrů IPv6 na síťových rozhraních,
- Směrování mezi jednotlivými rozhraními,
- Automatickou bezestavovou konfiguraci počítačů a zařízení v lokální síti (SLAAC),
- Základní firewall bez možnosti konfigurace (blokování komunikace směrem z Internetu do lokální sítě),
- Omezování šířky pásma (bez možnosti definice vlastních pravidel a rezervace šířky pásma),
- Přehled aktivních spojení,
- Objem přenesených dat na jednotlivých síťových rozhraních,
- Sledování IP komunikace v záznamu Debug.

Kerio Control tedy může fungovat jako IPv6 směrovač a umožňuje přístup z počítačů v lokální síti do Internetu s použitím protokolu IPv6.

Ostatní funkce a služby Kerio Control včetně administračního rozhraní jsou k dispozici pouze s použitím protokolu IPv4.

Kapitola 7

Síťová rozhraní

Kerio Control 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*, *Wi-Fi*, vytáčené linky atd.), která jsou do těchto sítí připojena.

Kerio Control 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 ve WWW rozhraní *Administration* v sekci *Konfigurace* → *Rozhraní*.

> ***Tip***
> Síťová rozhraní a některé další základní parametry *Kerio Control* lze snadno nastavit s použitím *Průvodce připojením* (viz kapitola 8.1). Tohoto průvodce lze spustit tlačítkem *Nastavit pomocí průvodce* v sekci *Rozhraní* nebo z *Konfiguračního asistenta* (viz kapitola 4.2) na úvodní stránce administračního rozhraní. Průvodce připojením však nepodporuje konfiguraci protokolu IPv6.

7.1 Skupiny rozhraní

Pro snazší konfiguraci firewallu a lepší přehlednost se síťová rozhraní v *Kerio Control* řadí do skupin. V komunikačních pravidlech firewallu lze skupiny rozhraní použít v položkách *Zdroj* a *Cíl*, stejně jako jednotlivá rozhraní (podrobnosti viz kapitola 9.3). Hlavní výhodou skupin rozhraní je fakt, že při změně internetového připojení, přidání nové linky, výměně síťového adaptéru atd. není vůbec nutné zasahovat do komunikačních pravidel — stačí pouze zařadit nové rozhraní do správné skupiny.

V *Kerio Control* 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 *Wi-Fi*),

[3] Chceme-li na systému *Windows* docílit toho, aby *Kerio Control* nepracoval s některým rozhraním, je možné ve vlastnostech tohoto rozhraní vypnout komponentu *Kerio Control* (nízkoúrovňový ovladač *Kerio Control*).
Z důvodu zajištění bezpečnosti a plné kontroly nad síťovou komunikací procházející přes firewall však doporučujeme nevypínat nízkoúrovňový ovladač *Kerio Control* na žádném síťovém rozhraní!
Kerio Control v edicích *Appliance* a *Box* pracuje vždy se všemi síťovými rozhraními, která jsou ve stavu „UP“.

- *Rozhraní pro VPN* — virtuální síťová rozhraní využívaná proprietárním řešením *Kerio VPN* (VPN server a vytvořené VPN tunely — podrobnosti viz kapitola 25),
- *Ostatní rozhraní* — rozhraní, která logicky nepatří do žádné z výše uvedených skupin (např. síťový adaptér pro demilitarizovanou zónu, 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 připojením* (viz kapitola 8.1) 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 firewallu 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.

7.2 Konfigurace portů Ethernet

Zařízení *Kerio Control Box* disponuje čtyřmi, resp. osmi porty Gigabit Ethernet. Jednotlivé porty mohou být softwarově nastaveny jako samostatná rozhraní nebo zařazeny do switche, případně vypnuty. V malých sítích tedy *Kerio Control* může sloužit nejen pro zabezpečení internetové brány, ale také jako switch — není potřeba žádné další zařízení. Ve složitějších síťových konfiguracích je možné využít virtuální sítě (VLAN).

Možnosti konfigurace portů Ethernet:

- *Samostatné rozhraní* — port bude použit jako samostatné rozhraní typu Ethernet.

  Takový port se obvykle využívá pro připojení k Internetu (zařadíme jej do skupiny *Internetová rozhraní*), případně připojení odděleného segmentu lokální sítě (skupina *Důvěryhodná / Lokální rozhraní*) nebo demilitarizované zóny (skupina *Ostatní rozhraní*).

- *Switch pro LAN* — port bude součástí switche, který se v *Kerio Control* chová jako jedno rozhraní typu *Ethernet*.

  Switch je standardně zařazen do skupiny *Důvěryhodná / Lokální rozhraní* a slouží pro připojení lokálních pracovních stanic, serverů, switchů, routerů a dalších zařízení, která tvoří infrastrukturu lokální sítě.

- *Nepřiřazeno* — port bude neaktivní. Toho lze využít např. pro dočasné odpojení počítače nebo části sítě, která je k tomuto portu připojena.

Rychlost a duplexní režim

Ve většině případů se propojená zařízení „dohodnou“ na rychlosti a režimu komunikace automaticky. Pokud je to z nějakého důvodu potřeba, je možné ručně zvolit požadovaný režim a rychlost.

Přiřazení portu

Port může mít jednu z následujících rolí:

- *Samostatné rozhraní* — port bude použit jako samostatné rozhraní typu Ethernet.
  Takový port se obvykle využívá pro připojení k Internetu (bude zařazen do skupiny *Internetová rozhraní*), případně připojení odděleného segmentu lokální sítě (skupina *Důvěryhodná / Lokální rozhraní*) nebo demilitarizované zóny (skupina *Ostatní rozhraní*).
- *Switch pro LAN* — port bude součástí switche, který se v Kerio Control chová jako jedno rozhraní typu Ethernet.
  Switch je standardně zařazen do skupiny *Důvěryhodná / Lokální rozhraní* a slouží pro připojení lokálních pracovních stanic, serverů, switchů, routerů a dalších zařízení, která tvoří infrastrukturu lokální sítě.
- *Nepřiřazeno* — port bude neaktivní. Toho lze využít např. pro dočasné odpojení počítače nebo části sítě, která je k tomuto portu připojena.

Virtuální lokální sítě (VLAN)

Na rozhraní typu Ethernet můžete vytvořit jednu nebo více tagovaných virtuálních sítí (VLAN, dle standardu IEEE 802.1Q).
Pro definici VLAN stačí uvést seznam jejich identifikátorů (VLAN ID). VLAN ID je celé číslo z rozsahu 1-4094. Jednotlivé identifikátory se oddělují středníky. Na každém rozhraní lze definovat nejvýše 1000 VLAN.
Každá VLAN se v Kerio Control chová jako samostatné rozhraní typu Ethernet. Nově definované VLAN jsou automaticky zařazeny do skupiny *Ostatní rozhraní*.
Role fyzického portu (samostatné rozhraní / switch / nepřiřazeno) nemá na VLAN žádný vliv.

Kerio Control Appliance Edition

Edice Appliance (Software Appliance nebo virtuální zařízení) umožňuje nastavení rychlosti a duplexního režimu rozhraní typu Ethernet a vytváření virtuálních sítí (VLAN) na těchto rozhraních.

Fyzická rozhraní (porty) nelze zařadit do switche.

Edice pro systém Windows

V edici pro systém Windows není možné konfigurovat porty Ethernet ani vytvářet virtuální sítě (VLAN).

7.3 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/control/download). VPN server je vždy zařazen do skupiny *Rozhraní pro VPN*. Rozhraní *VPN server* nelze odstranit.

Podrobné informace o proprietárním VPN řešení *Kerio VPN* naleznete v kapitole 25.

Dial-In (pouze na systému Windows)

Toto rozhraní představuje server služby *RAS* (telefonického připojení sítě) na počítači s *Kerio Control*. S použitím rozhraní *Dial-In* lze definovat komunikační pravidla (viz kapitola 9) 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 nepovažujete za součást důvěryhodné lokální sítě, přesuňte rozhraní *Dial-In* přesunout do skupiny *Ostatní rozhraní*.

Poznámka:

1. Při použití RAS serveru společně s *Kerio Control* je třeba nastavit RAS server tak, aby přiděloval klientům IP adresy ze subsítě, která není použita v žádném segmentu lokální sítě. *Kerio Control* 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 *Kerio Control* *nelze* využít DHCP server v *Kerio Control*. Podrobnosti viz kapitola 11.2.

7.4 Zobrazení a změna parametrů rozhraní

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

Jméno

Jednoznačný název, který identifikuje rozhraní v rámci *Kerio Control*. 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 *Kerio Control*.

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*).

Stav
Stav rozhraní (připojeno/odpojeno).

IPv4 adresa, maska, brána, DNS
Parametry protokolu IPv4.

IPv6 adresa, délka prefixu, brána
Parametry protokolu IPv6.

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.

Připojení
Informace o tom, jakým způsobem je rozhraní použito pro internetové připojení:

- Zálohované připojení — primární nebo sekundární linka,
- Rozložení zátěže sítě — váha linky.

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.

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 / Přidat → VPN tunel
Tímto tlačítkem lze vytvořit nový VPN tunel typu server-to-server. Podrobnosti o proprietárním VPN řešení *Kerio VPN* viz kapitola 25.
Poznámka:
V edicích *Appliance* a *Box* je možné také přidávat nová rozhraní (PPTP a PPPoE připojení) — viz sekce 7.5. Je-li *Kerio Control* 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.
Každému rozhraní lze v *Kerio Control* 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), nastavení výchozí brány a DNS serverů.
V edicích *Appliance* a *Box* je možné v tomto dialogu nastavit všechny parametry síťového rozhraní. Rozhraní mohou být přiřazeny další IP adresy (v případě protokolu IPv4 lze

přidat maximálně přidat 32 sekundárních IP adres; počet sekundárních IPv6 adres není omezen).
Jedná-li se o vytáčenou linku, umožňuje dialog nastavit také přihlašovací údaje a volby pro vytáčení (viz kapitola 8.5).
V případě rozhraní *VPN server* a VPN tunelů se zobrazí dialog pro nastavení parametrů VPN serveru (viz kapitola 25.1), resp. VPN tunelu (viz kapitola 25.3).

Odebrat

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

- jedná se o neaktivní (odpojený) 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 *Kerio Control* nepovolí odebrat.
Poznámka:

1. Záznam o již neexistujícím síťovém adaptéru nebo odstraněné vytáčené lince nemá žádný vliv na činnost *Kerio Control* — 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 9.3).

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 18.2 a manuál *Kerio Control — Příručka uživatele*).
- V případě VPN tunelu jsou tato tlačítka označena *Povolit* a *Zakázat* a slouží k aktivaci / deaktivaci vybraného VPN tunelu (podrobnosti viz kapitola 25.3).
  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.

7.5 Přidání nového rozhraní (edice Appliance a Box)

Kerio Control v edicích *Appliance* a *Box* umožňuje přidávat nová síťová rozhraní (PPTP a PPPoE připojení).

Stisknutím tlačítka *Přidat* se zobrazí nabídka, ze které vybereme požadovaný typ nového rozhraní.

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

Dále jsou vyžadovány údaje podle typu připojení:

- *PPTP* — PPTP server, uživatelské jméno a heslo,
- *PPPoE* — rozhraní (typu Ethernet), uživatelské jméno a heslo. Rozhraní může být nastaveno jako libovolné — *Kerio Control* pak automaticky vybere vhodné rozhraní, přes které bude PPPoE připojení navázáno.

—

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 nutné linku vytáčet ručně (buď v administračním rozhraní nebo v uživatelském WWW rozhraní — viz manuál *Kerio Control — Příručka uživatele*). Linka může být automaticky zavěšována po nastavené době nečinnosti (podrobnosti viz sekce 7.6).

Poznámka:
Připojení typu PPPoE lze rovněž definovat ve vlastnostech příslušného rozhraní typu *Ethernet*. To je doporučený způsob, pokud budete využívat pouze jedno PPPoE připojení přes vyhrazené rozhraní.

7.6 Upřesňující nastavení vytáčené linky

Pro vytáčené linky je dialog pro nastavení parametrů rozhraní (viz kapitola 7) 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).

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 nutné linku připojovat ručně (buď v administračním rozhraní nebo v uživatelském WWW rozhraní — viz manuál *Kerio Control — Příručka uživatele*). *Kerio Control* na systému *Windows* podporuje také režim automatického vytáčení linky na základě požadavků z lokální sítě (tzv. vytáčení na žádost — viz kapitola 8.5).

Poznámka:

1. Pokud je ve směrovací tabulce v *Kerio Control* 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 20.1.
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).

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

7.7 Pomocné skripty pro ovládání linky (Windows)

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.

Kerio Control umožňuje spustit libovolný program nebo příkaz v těchto okamžicích: *Před vytočením* linky, *Po vytočení* linky, *Před zavěšením* linky a *Po zavěšení* linky. V případě akcí *Před vytočením* a *Před zavěšením* se po spuštění programu nečeká na jeho ukončení.

Skripty pro ovládání vytáčených linek musejí být umístěny v podadresáři `scripts` instalačního adresáře firewallu, typicky

```
C:\Program Files\Kerio\WinRoute Firewall\scripts
```

(pozor, tento adresář ve výchozí instalaci neexistuje — je potřeba jej vytvořit!).

Soubory skriptů musejí mít tyto názvy:

- `BeforeDial.cmd` — před vytočením linky,
- `AfterDial.cmd` — po vytočení linky,
- `BeforeHangup.cmd` — před zavěšením linky,
- `AfterHangup.cmd` — po zavěšení linky.

Každému skriptu je jako první parametr předán celý název připojení, které je právě vytáčeno nebo zavěšováno — jméno rozhraní v *Kerio Control*.

Případné chyby (např. pokud povolíme některou akci, ale příslušný skript neexistuje) se zapisují do záznamu *Error* (viz kapitola 24.8).

Poznámka:
Pokud název vytáčeného připojení obsahuje mezery, bude při volání skriptu automaticky vložen do uvozovek, čímž bude správně zajištěno předání celého názvu v jediném parametru skriptu. Vhodnější je však používat pro vytáčená rozhraní názvy bez mezer a bez diakritiky. Rozhraní v *Kerio Control* lze kdykoliv bez problémů přejmenovat.

Upozornění:
V operačním systému *Windows* běží *Kerio Control* 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. V některých případech by taková aplikace mohla zároveň blokovat další vytočení nebo zavěšení linky.

Kapitola 8

Nastavení internetového připojení a lokální sítě

Základní funkcí *Kerio Control* je připojení lokální sítě k Internetu.

Pro sítě používající protokol IPv4 je možné použít jedno nebo více internetových připojení (internetových linek). V závislosti na počtu a typu linek nabízí *Kerio Control* různé možnosti připojení k Internetu. V případě protokolu IPv6 je možné připojení pouze jednou linkou.

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

Jedna linka — vytáčení na žádost (pouze na systému Windows)
: 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 *Kerio Control* ji automaticky vytočí v okamžiku, kdy zaznamená požadavek na přístup z lokální sítě do Internetu. Pokud nejsou po lince přenášena žádná data, *Kerio Control* ji po nastavené době opět zavěsí, čímž snižuje náklady na připojení.
Tento režim je k dispozici pouze v *Kerio Control* pro systém Windows. *Kerio Control* v edicích *Appliance* a *Box* nepodporuje vytáčené linky.

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 *Kerio Control* automaticky používat záložní linku (pevnou nebo vytáčenou). Uživatelé tak zaznamenají jen velmi krátkodobý výpadek internetového připojení. Po obnovení funkčnosti primární linky *Kerio Control* 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 *Kerio Control* 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.

Při konfiguraci internetového připojení v *Kerio Control* 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 9.3).

8.1 Průvodce připojením

Pro snadnou konfiguraci síťových rozhraní, internetového připojení a lokální sítě nabízí *Kerio Control* tzv. *Průvodce připojením*. Tohoto průvodce lze spustit z *Konfiguračního asistenta* (viz kapitola 4.2) nebo tlačítkem *Nastavit pomocí průvodce* v sekci *Konfigurace* → *Rozhraní*.

Typické použití průvodce připojením je počáteční konfigurace internetového připojení a lokální sítě. Při pozdějším použití se průvodce snaží do maximální možné míry respektovat stávající konfiguraci firewallu. Pokud detekuje specifická nastavení, se kterými by nemohl pracovat, zobrazí podrobné informace a ukončí se. Správce *Kerio Control* pak může tato nastavení ručně upravit nebo provést potřebné konfigurační změny bez použití průvodce. Mezi tato „nepodporovaná“ nastavení patří např. DHCP server v režimu ruční konfigurace (viz kapitola 11.2) nebo vytáčení internetového připojení na žádost (*Kerio Control* na systému Windows).

Režim internetového připojení

Prvním krokem průvodce je výběr režimu internetového připojení:

- *Jedna internetová linka* — připojení jednou pevnou nebo vytáčenou linkou (viz kapitola 8.2).
- *Dvě internetové linky s rozložením zátěže* — pro připojení k Internetu budou použity dvě linky, čímž se zvýší rychlost (propustnost) připojení (viz kapitola 8.3).
- *Dvě internetové linky se zálohováním* — pro připojení k Internetu bude použita jedna (primární) linka, při výpadku se automaticky přepne na druhou (záložní) linku (viz kapitola 8.4).

Jednotlivé režimy připojení jsou podrobně popsány v následujících kapitolách.

Poznámka:

1. Průvodce umožňuje nastavit pouze parametry protokolu IPv4. Chcete-li používat protokol IPv6, je potřeba nastavit parametry jednotlivých síťových rozhraní ručně.
2. Režimy rozložení zátěže a zálohování připojení lze použít pouze s protokolem IPv4.
3. *Kerio Control* na systému *Windows* umožňuje také vytáčení internetového připojení na žádost. Tento režim nelze nastavit pomocí průvodce. Podrobnosti viz kapitola 8.5.

Výběr internetových rozhraní

V závislosti na zvoleném režimu připojení je potřeba vybrat rozhraní připojené (resp. připojená) k Internetu.

Průvodce umožňuje u jednotlivých rozhraní upravit nastavení výchozí brány a DNS serverů (standardně se používá nastavení detekované z operačního systému firewallu).

Kerio Control v edicích *Appliance* a *Box* umožňuje nastavit také IP adresu a masku subsítě na jednotlivých rozhraní.

V průvodci není možné nastavit parametry vytáčeného připojení (telefonní číslo, přihlašovací údaje atd.).

Výběr rozhraní pro lokální síť a nastavení DHCP serveru

Dalším krokem je výběr rozhraní připojeného k lokální síti.

Rozhraní pro lokální síť bude sloužit jako výchozí brána (případně i jako DNS server) pro počítače v lokální síti. Z tohoto důvodu musí mít rozhraní pevnou IP adresu a nelze jej tedy konfigurovat protokolem DHCP.

Průvodce předpokládá, že je k lokální síti právě jedno rozhraní firewallu. Rozhraní nepoužitá pro internetové připojení ani pro lokální síť budou zařazena do skupiny *Ostatní rozhraní*. Je-li lokální síť tvořena více segmenty připojenými k různým rozhraním firewallu, pak stačí po dokončení průvodce přidat všechna zbývající rozhraní do skupiny *Důvěryhodná / Lokální rozhraní*.

Současně s výběrem rozhraní pro lokální síť je možné také povolit automatickou konfiguraci počítačů v lokální síti DHCP serverem v *Kerio Control* (doporučeno). Tato volba zapne DHCP server v režimu automatické konfigurace — není potřeba nic dalšího nastavovat. Nechcete-li DHCP server v *Kerio Control* použít, ponechá jej průvodce vypnutý, aby nedocházelo ke kolizím.

Shrnutí a aplikace nové konfigurace

V posledním kroku průvodce se zobrazí shrnutí nové konfigurace připojení na základě zadaných informací.

Toto je poslední možnost, kdy lze průvodce přerušit. Po potvrzení bude nová konfigurace aplikována.

8.2 Připojení k Internetu jednou linkou

Požadavky

Počítač s *Kerio Control* musí být připojen k Internetu pevnou linkou (typicky adaptér *Ethernet* nebo *Wi-Fi*). 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 — typicky připojení *PPPoE*. Linku tohoto typu bude *Kerio Control* 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!

> ***Tip***
> Na systému *Windows* doporučujeme vyzkoušet funkčnost internetového připojení ještě před instalací *Kerio Control*.

Konfigurace pomocí průvodce

1. V prvním kroku *Průvodce připojením* (viz kapitola 9.1) zvolíme možnost *Jedna internetová linka*.

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

   Průvodce umožňuje upravit nastavení výchozí brány a DNS serverů na vybraném rozhraní. V edicích *Appliance* a *Box* je možné nastavit také IP adresu a masku subsítě.

   Pokud zvolíme připojení *PPPoE*, pak je potřeba zadat příslušné uživatelské jméno a heslo.

   Poznámka:
   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.

   Podrobné informace o síťových rozhraních naleznete v kapitole 7.

3. Ve třetím kroku průvodce zvolíme rozhraní připojené k lokální síti. Je-li k lokální síti připojeno více rozhraní, vybereme v průvodci rozhraní, přes které jsme aktuálně připojeni ke správě *Kerio Control*. Zbývající adaptéry pak ručně přesuneme do skupiny *Důvěryhodná / Lokální rozhraní*.

Výsledná konfigurace rozhraní

Do skupiny *Internetová rozhraní* je zařazen pouze adaptér *Internet* vybraný ve druhém kroku průvodce. Do skupiny *Důvěryhodná / Lokální rozhraní* je zařazen pouze adaptér *LAN* zvolený ve třetím kroku průvodce.

Zbývající rozhraní jsou považována za nepoužitá a jsou zařazena do skupiny *Ostatní rozhraní*. Pro tato rozhraní je pak nutné ručně definovat odpovídající komunikační pravidla (např. pro vytvoření demilitarizované zóny — viz kapitola 9.5). Pokud nastavení rozhraní neodpovídá

skutečné konfiguraci sítě, upravte konfiguraci rozhraní (např. pokud má firewall více rozhraní pro lokální síť, přesuňte příslušná rozhraní do skupiny *Důvěryhodná / Lokální rozhraní*).

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 20.1) 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 *Kerio Control* 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.

8.3 Rozložení zátěže internetového připojení

Jsou-li k dispozici alespoň dvě internetové linky, může *Kerio Control* 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 9.6), pak jsou jednotlivé linky navíc vzájemně zálohovány (viz též kapitola 8.4) — 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 20.1) 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 *Kerio Control* musí mít dvě síťová rozhraní pro připojení k Internetu, a to pevné linky (*Ethernet*, *Wi-Fi*) nebo trvale připojené vytáčené linky (*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!

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

Tip
Na systému *Windows* doporučujeme prověřit funkčnost jednotlivých internetových linek ještě před instalací *Kerio Control*. Možné způsoby testování (pro dvě linky):

- Pokud se jedná o dvě linky vytáčeného charakteru, připojte 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

1. V prvním kroku *Průvodce připojením* (viz kapitola 9.1) zvolíme možnost *Dvě internetové linky s rozložením zátěže*.

2. Ve druhém kroku průvodce pak postupně vybereme dvě rozhraní, které chceme použít jako internetové linky pro rozložení zátěže připojení. Pokud zvolíme připojení *PPPoE*, pak je potřeba zadat příslušné uživatelské jméno a heslo.

   Pro každou linku je třeba specifikovat váhu linky, tj. její relativní propustnost. Poměr vah jednotlivých linek udává, jakým způsobem bude internetová komunikace mezi tyto linky rozdělována (měl by tedy odpovídat poměru jejich rychlostí).

   Příklad
   Máme k dispozici dvě internetové linky o rychlostech *4 Mbit/s* a *8 Mbit/s*. První lince nastavíme váhu *10* a druhé váhu *20*. Celková zátěž internetového připojení tedy bude rozdělena v poměru 1:2.

   Podrobné informace o síťových rozhraních naleznete v kapitole 7.

3. Ve třetím kroku průvodce zvolte rozhraní připojené k lokální síti. Je-li k lokální síti připojeno více rozhraní, vyberte v průvodci rozhraní, přes které jste aktuálně připojeni ke správě *Kerio Control*. Zbývající adaptéry pak ručně přesuňte do skupiny *Důvěryhodná / Lokální rozhraní*.

Výsledná konfigurace rozhraní

Do skupiny *Internetová rozhraní* jsou zařazeny dvě internetové linky vybrané ve třetím kroku průvodce.

Ve sloupci *Připojení* se zobrazují nastavené váhy 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.

Při přidání další linky do skupiny *Internetová rozhraní* bude nové lince nastavena výchozí váha (*1*). Pak je vhodné upravit v dialogu pro změnu parametrů rozhraní (viz kapitola 7) váhu linky s ohledem na její skutečnou rychlost, aby byla zátěž rozložena pokud možno rovnoměrně.

Do skupiny *Důvěryhodná / Lokální rozhraní* je zařazen pouze adaptér *LAN* zvolený ve třetím kroku průvodce.

Zbývající rozhraní jsou považována za nepoužitá a jsou zařazena do skupiny *Ostatní rozhraní*. Pro tato rozhraní je pak nutné ručně definovat odpovídající komunikační pravidla (např. pro vytvoření demilitarizované zóny — viz kapitola 9.5). Pokud nastavení rozhraní neodpovídá skutečné konfiguraci sítě, upravte konfiguraci rozhraní (např. pokud má firewall více rozhraní pro lokální síť, přesuňte příslušná rozhraní do skupiny *Důvěryhodná / Lokální rozhraní*).

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 9.6.

Upřesňující parametry

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.

Poznámka:

1. Testovací počítač nesmí blokovat zprávy *ICMP Echo Request* (*PING*), které *Kerio Control* 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.).
3. *ICMP* zprávy odesílané na testovací počítače nelze zablokovat komunikačními pravidly firewallu.

VPN tunely

Při obnovení připojení přes primární linku může *Kerio Control* automaticky odpojit a znovu připojit všechny VPN tunely. Je-li tato volba vypnuta, VPN tunely zůstanou navázané přes záložní linku a není zaručena správna funkčnost směrování mezi privátními sítěmi.

8.4 Zálohované internetové připojení

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

Požadavky

Počítač s *Kerio Control* musí mít dvě síťová rozhraní pro připojení k Internetu: pevnou linku (*Ethernet*, *Wi-Fi*) nebo trvale připojenou vytáčenou linku (*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!

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

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.

Tip
Na systému *Windows* doporučujeme prověřit funkčnost primární a sekundární linky ještě před instalací *Kerio Control*:

- 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.

Konfigurace pomocí průvodce

1. V prvním kroku *Průvodce připojením* zvolíme možnost *Dvě internetové linky se zálohováním*.
2. Ve druhém kroku průvodce pak vybereme síťové rozhraní pro primární připojení (pevnou nebo trvale připojenou linku) a pro sekundární připojení (pevnou nebo vytáčenou linku). Pokud zvolíte připojení *PPPoE*, pak je potřeba zadat příslušné uživatelské jméno a heslo.

   Průvodce umožňuje upravit nastavení výchozí brány a DNS serverů na vybraném rozhraní. V edicích *Appliance* a *Box* je možné nastavit také IP adresu a masku subsítě. Pokud zvolíme připojení *PPPoE*, pak je potřeba zadat příslušné uživatelské jméno a heslo.

   Podrobné informace o síťových rozhraních naleznete v kapitole 7.
3. Ve třetím kroku průvodce zvolíme rozhraní připojené k lokální síti. Je-li k lokální síti připojeno více rozhraní, vybereme v průvodci rozhraní, přes které jsme aktuálně připojeni ke správě *Kerio Control*. Zbývající adaptéry pak ručně přesuneme do skupiny *Důvěryhodná / Lokální rozhraní*.

Výsledná konfigurace rozhraní

Do skupiny *Internetová rozhraní* jsou zařazeny linky *Internet* a *Vytáčené připojení* vybrané ve druhém 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.

Do skupiny *Důvěryhodná / Lokální rozhraní* je zařazen pouze adaptér *LAN* zvolený ve třetím kroku průvodce.

Zbývající rozhraní jsou považována za nepoužitá a jsou zařazena do skupiny *Ostatní rozhraní*. Pro tato rozhraní je pak nutné ručně definovat odpovídající komunikační pravidla (např. pro vytvoření demilitarizované zóny — viz kapitola 9.5). Pokud nastavení rozhraní neodpovídá skutečné konfiguraci sítě, upravíme konfiguraci rozhraní (např. pokud má firewall více rozhraní pro lokální síť, přesuneme příslušná rozhraní do skupiny *Důvěryhodná / Lokální rozhraní*).

Chceme-li změnit nastavení primárního a sekundárního připojení, použijeme volby v dialogu pro změnu parametrů rozhraní (viz kapitola 7) 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.

Upřesňující parametry

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.

Poznámka:

1. Testovací počítač nesmí blokovat zprávy *ICMP Echo Request* (*PING*), které *Kerio Control* 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.

VPN tunely

Při obnovení připojení přes primární linku může *Kerio Control* automaticky odpojit a znovu připojit všechny VPN tunely. Je-li tato volba vypnuta, VPN tunely zůstanou navázané přes záložní linku a není zaručena správna funkčnost směrování mezi privátními sítěmi.

8.5 Připojení jednou vytáčenou linkou - vytáčení na žádost (Windows)

Je-li počítač s *Kerio Control* 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). *Kerio Control* na systému *Windows* nabízí možnost automatického vytáčení linky na základě požadavků z lokální sítě. Tato funkce se nazývá vytáčení na žádost.

Poznámka:
V edicích *Appliance* a *Box* není vytáčení na žádost podporováno.

Požadavky

V počítači s *Kerio Control* 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 v *Kerio Control*. 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 *Kerio Control*.

> ***Upozornění:***
> Před konfigurací lokální sítě a firewallu s použitím internetové linky vytáčené na žádost doporučujeme důkladně prostudovat informace uvedené v kapitole 27.6. Vhodným návrhem konfigurace sítě s ohledem na specifické vlastnosti linky vytáčené na žádost lze předejít mnoha pozdějším problémům.

Konfigurace

Režim vytáčení na žádost nelze nastavit pomocí průvodce připojením — síťová rozhraní nastavíme ručně v sekci *Konfigurace / Rozhraní*.

Do skupiny *Internetová rozhraní* zařadíme linku *Vytáčené připojení*. Ve vlastnostech rozhraní musíme označit, že toto rozhraní má být použito jako linka vytáčená na žádost (tato informace se pak zobrazí ve sloupci *Internet*).

Do skupiny *Důvěryhodná / Lokální rozhraní* zařadíme všechna rozhraní připojená k lokální síti.

Zbývající rozhraní zůstanou zařazena do skupiny *Ostatní rozhraní*. Pro tato rozhraní je pak nutné ručně definovat odpovídající komunikační pravidla (např. pro vytvoření demilitarizované zóny — viz kapitola 9.5).

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 *Kerio Control* směrovat pakety do příslušné cílové sítě dle systémové směrovací tabulky (viz též kapitola 20.1) 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 7) 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 *Kerio Control* vytvoří výchozí cestu vytočením internetové linky).

Podrobné informace o síťových rozhraních naleznete v kapitole 7.

Upřesňující nastavení vytáčení

Tlačítkem *Upřesnění* lze nastavit parametry pro vytáčení linky — např. intervaly, kdy má být linka trvale připojena nebo naopak trvale zavěšena, a pomocné skripty pro vytáčení a zavěšování linky. Tato nastavení jsou podrobně popsána v kapitole 7.6.

Kapitola 9

Komunikační pravidla

Komunikační pravidla (*Traffic Rules*) jsou základem konfigurace *Kerio Control*. V jediné tabulce je integrováno nastavení:

- zabezpečení (tj. ochrany lokální sítě včetně počítače, na němž je *Kerio Control* 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* → *Zásady komunikace* → *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.

Komunikační pravidla pracují pouze nad protokolem IPv4. V případě protokolu IPv6 je implicitně povolena komunikace zahájená z lokální sítě a zakázána komunikace zahájená z Internetu směrem do lokální sítě (implicitní firewall).

9.1 Průvodce komunikačními pravidly

Průvodce komunikačními pravidly se spustí stisknutím tlačítka *Nastavit pomocí průvodce* v sekci *Konfigurace* → *Zásady komunikace* → *Komunikační pravidla*.

Průvodce 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 *Kerio Control*) proti neoprávněnému přístupu z Internetu.

Podmínky použití průvodce

Průvodce předpokládá, že je počítač (resp. zařízení) s *Kerio Control* vybaven:

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

Krok 1 — potvrzení

Aby bylo možné zaručit funkčnost *Kerio Control* po použití průvodce, jsou před dokončením průvodce všechna stávající pravidla smazána a nahrazena pravidly vytvořenými automaticky na základě poskytnutých informací. Pokud se nejedná o počáteční konfiguraci (bezprostředně po instalaci *Kerio Control*), pak se průvodce v prvním kroku dotáže, zda skutečně chcete přepsat stávající komunikační pravidla.

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 2 — zpřístupnění služeb Kerio Control z Internetu

Ve druhém kroku průvodce vyberte služby *Kerio Control*, které mají být dostupné z Internetu:

- *Kerio VPN server* — připojení k VPN serveru v *Kerio Control*. Povolte tuto službu, pokud chcete vytvářet VPN tunely a/nebo se připojovat vzdáleně do lokální sítě pomocí aplikace *Kerio VPN Client*. Bližší informace viz kapitola 25.
- *Server Kerio SSL-VPN (HTTPS)* — rozhraní *Kerio Clientless SSL-VPN* (k dispozici pouze v *Kerio Control* na systému Windows). Tato volba povolí komunikaci protokolem HTTPS na standardním portu (`443`). Bližší informace viz kapitola 26.
- *Kerio Control Administration* — povolení vzdálené správy *Kerio Control*. Tato volba povolí komunikaci protokolem HTTPS na portu `4081` (port administračního rozhraní nelze změnit).

Krok 3 — zpřístupnění (mapování) dalších služeb

Ve třetím kroku průvodce je možné zpřístupnit z Internetu (mapovat) libovolné další služby na firewallu nebo na serverech v lokální síti.

Každá položka (mapovací pravidlo) obsahuje:

- Mapovanou službu — buď lze vybrat ze seznamu definovaných služeb (viz kapitola 17.3) nebo je možné zadat službu protokolem a číslem portu.
- Cílový počítač — firewall nebo IP adresa lokálního serveru, na kterém služba běží.

Pravidla vytvořená průvodcem

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

Služby na ...

Tato dvě pravidla uvádíme jako příklady mapovaných služeb na lokálních serverech. Pro každý lokální server bude vytvořeno jedno pravidlo ve tvaru *Služby na <IP adresa serveru>*, resp. *Služby na firewallu*.

Tyto služby budou přístupné na všech IP adresách všech „vnějších" rozhraní firewallu (tj. rozhraní ve skupině *Internetová rozhraní*).

Kerio Control Administration, Kerio VPN Server, Clientless SSL-VPN

Tato pravidla povolují přístup ke správě *Kerio Control*, VPN serveru a rozhraní *Kerio Clientless SSL-VPN*. Jednotlivá pravidla jsou vytvořena pouze pokud byly příslušné služby vybrány ve druhém kroku průvodce.

Přístup do Internetu (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.

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.

Poznámka:

Na systému *Windows* 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 *Kerio Control* nainstalován). Položky *Zdroj* a *Cíl* v tomto pravidle zahrnují skupinu *Důvěryhodná / Lokální rozhraní* (viz kapitola 7) a speciální skupinu *Firewall*.

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 v *Kerio Control*.

Poznámka:

1. Průvodce předpokládá, že firewall 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 firewallu může mít za následek zablokování vzdálené správy či nedostupnost

služeb v Internetu (prochází přes něj veškerá komunikace mezi lokální sítí a Internetem).
2. Na systému Windows 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.

Komunikace firewallu
Toto pravidlo povoluje přístup k vybraným službám z počítače, kde je *Kerio Control* 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 naleznete v kapitole 9.3.

9.2 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 v *Kerio Control* 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 *Kerio Control* k tomuto účelu nabízí — viz kapitola 15.

9.3 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.

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

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).

Poznámka:
Jméno 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:

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

  Je-li zdrojový nebo cílový počítač zadán DNS jménem, pak *Kerio Control* zjišťuje odpovídající IP adresu v okamžiku stisknutí tlačítka *Použít*. Pokud není nalezen záznam v cache modulu *DNS*, vysílá se DNS dotaz do Internetu. Do zjištění IP adresy je příslušné pravidlo neaktivní.

- *Rozsah IP adres* — např. `192.168.1.10—192.168.1.20`

- *Subsíť s maskou* — subsíť zadaná adresou sítě a maskou

  (např. `192.168.1.0/255.255.255.0`)

- *Skupina IP adres* — skupina adres definovaná v *Kerio Control* (viz kapitola 17.1)

- *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 7.

V komunikačních pravidlech lze použít pouze skupiny *Internetová rozhraní* 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:

  1. *Příchozí spojení (VPN klienti)* — všichni VPN klienti připojující se k VPN serveru v *Kerio Control* 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 v *Kerio Control* naleznete v kapitole 25.

- *Libovolný ověřený uživatel* — podmínka bude platit pro všechny uživatele, kteří jsou na firewall již přihlášeni (viz kapitola 13.1). Volbou *Uživatelé z domény* můžeme přidat požadované uživatele a/nebo skupiny z mapovaných domén adresářových služeb nebo z lokální databáze uživatelů (podrobnosti viz kapitola 18).

- *Vybraní uživatelé / skupiny* — uživatelé a/nebo skupiny uživatelů, které lze vybrat ve speciálním dialogu.

> ***Tip***
> Do pravidla můžete přidat uživatele/skupiny z několika různých domén zároveň. Vyberte doménu, přidejte 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 13.1.

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 14 a 13.1) ve svém WWW prohlížeči a přihlásit se.
Tato problematika je podrobně diskutována v kapitole 9.7.

- *Firewall* — speciální skupina adres zahrnující všechna rozhraní počítače, na němž je *Kerio Control* nainstalován. Tuto volbu lze s výhodou využít např. pro povolení komunikace mezi lokální sítí firewallem.

Poznámka:
Při odstranění rozhraní, uživatelského účtu, skupiny nebo služby bude do odpovídající položky v příslušných pravidlech dosazena speciální hodnota *Nic* a tato pravidla budou neaktivní. Tím je zajištěno, že odebráním použité položky nedojde 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 17.3) a/nebo služeb zadaných protokolem a číslem portu (případně rozsahem portů — pro jeho specifikaci se zde používá pomlčka).

Poznámka:
Existuje-li v *Kerio Control* 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 9.8.

Akce, záznam a DSCP

Akce určuje způsob, jak *Kerio Control* obslouží komunikaci, která vyhoví podmínkám tohoto pravidla (podmínka je dána položkami *Zdroj*, *Cíl* a *Služba*):

- *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:
Při omezování lokálních uživatelů v přístupu na Internet doporučujeme používat volbu *Zakázat*, při blokování přístupu z Internetu naopak volbu *Zahodit*.

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

- *Graf přenesených dat* — časový průběh síťové komunikace. Tyto grafy se zobrazují v sekci *Stav* → *Grafy* (viz kapitola 22.2).
- *Zaznamenat pakety* — pakety, které vyhoví tomuto pravidlu (propuštěné, odmítnuté či zahozené — v závislosti na typu akce v pravidle) budou zaznamenány do záznamu *Filter*.
- *Zaznamenat spojení* — 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).

V povolené komunikaci mohou být odpovídající pakety označeny určitou hodnotou *DSCP*. Tato hodnota slouží k omezení šířky pásma (rychlosti přenosu dat) nebo naopak vyhrazení pásma pro danou komunikaci (viz kapitola 12). V „neoznačených“ paketech má tato položka hodnotu *0*.

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 9.4.

Pro překlad zdrojové adresy nabízí *Kerio Control* tyto možnosti:

Automatický výběr IP 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 9.4), protože funguje správně při libovolné konfiguraci internetového připojení a stavu jednotlivých linek (podrobnosti viz kapitola 8).
Pokud *Kerio Control* pracuje v režimu rozložení zátěže internetového připojení (viz kapitola 8.3), 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 *Kerio Control* 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 9.4.

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 9.6.
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. *Kerio Control* 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 *Kerio Control*. 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.

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 *Kerio Control* 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 *Kerio Control* 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 9.9.

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.

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 *Kerio Control* (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.

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

  > ***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 9.4.

Časová platnost

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

Speciální volba *Vždy* vypíná časové omezení pravidla (v okně *Komunikační pravidla* se pak nezobrazuje nic).

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:

- *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 *Kerio Control* 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 9.8.

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).

9.4 Základní typy komunikačních pravidel

Komunikační pravidla v *Kerio Control* 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 *Kerio Control*. 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
Přístup do Internetu (NAT)	Důvěryhodná / lokální rozhraní	Internetová rozhraní	Libovolný	Povolit	NAT Rozložení zátěže podle počítačů

Obrázek 9.1 Typické komunikační pravidlo pro překlad IP adres (sdílení internetového připojení)

Zdroj

Skupina *Důvěryhodná / Lokální rozhraní*. 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 20.1).

Cíl

Skupina rozhraní *Internet*. S použitím této skupiny je pravidlo univerzálně použitelné pro libovolný typ internetového připojení (viz kapitola 8) 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 *Kerio Control*. 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.

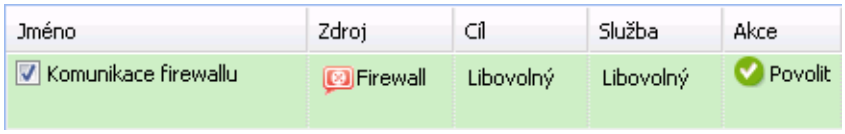
> ***Upozornění:***
> V sekci *Překlad cílové adresy* by měla být nastavena volba *Nepřekládat*, jinak není zaručena zamýšlená funkce pravidla. Kombinace překladu zdrojové i cílové adresy má význam pouze ve speciálních případech.

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 *Kerio Control* nainstalován)!

Komunikace mezi firewallem a Internetem musí být explicitně povolena samostatným pravidlem. Protože počítač s *Kerio Control* má přímý přístup do Internetu, není nutné použít překlad IP adres.



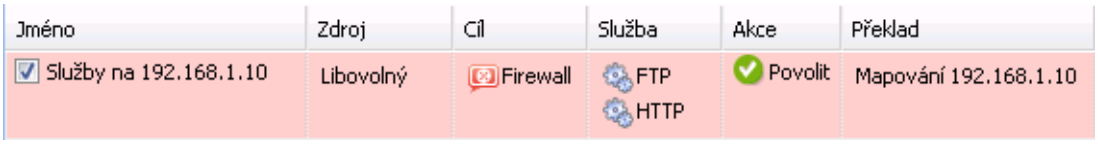
Obrázek 9.2 Pravidlo pro komunikaci firewallu s počítači v Internetu

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 *Kerio Control*.

Kerio Control 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 9.3 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 *Kerio Control*, 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 17.3) 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 *Kerio Control*. 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 `195.39.55.12` a `195.39.55.13`. Server `web1` má být z Internetu dostupný na IP adrese `195.39.55.12`, server `web2` na IP adrese `195.39.55.13`.

Pro splnění těchto požadavků definujeme v *Kerio Control* dvě komunikační pravidla:

Jméno	Zdroj	Cíl	Služba	Akce	Překlad
Mapování serveru web1	Libovolný	195.39.55.12	HTTP	Povolit	Mapování 192.168.1.100
Mapování serveru web2	Libovolný	195.39.55.13	HTTP	Povolit	Mapování 192.168.1.200

Obrázek 9.4 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).

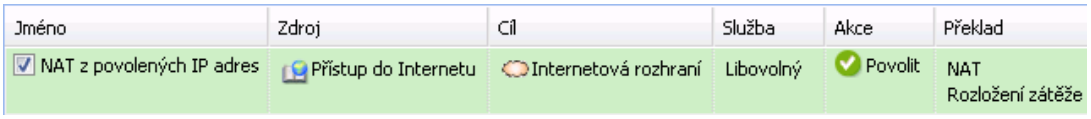
Poznámka:
Pravidla uvedená v těchto příkladech mohou být také použita, jestliže je *Kerio Control* nasazen jako tzv. neutrální směrovač (tj. směrovač bez překladu IP adres) — pouze v položce *Překlad* nebude žádný překlad definován.

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

Jméno	Zdroj	Cíl	Služba	Akce	Překlad
Přístup do Internetu (NAT)	Důvěryhodná / lokální rozhraní	Internetová rozhraní	DNS FTP FTPS HTTP HTTPS SSH	Povolit	NAT Rozložení zátěže

Obrázek 9.5 Sdílení internetového připojení — povolení přístupu pouze k vybraným službám

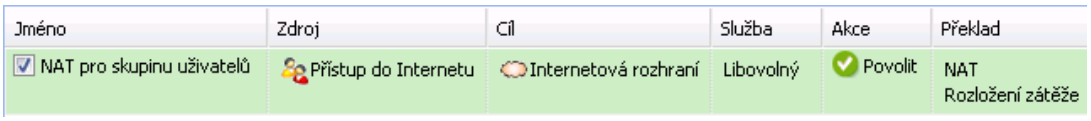
2. Omezení dle IP adres. Přístup k určitým službám (případně kompletní přístup do Internetu) bude povolen pouze z vybraných počítačů. V položce *Zdroj* definovaného pravidla uvedeme skupinu IP adres, ze kterých bude přístup do Internetu povolen. Tuto skupinu je třeba nejprve definovat v sekci *Konfigurace* → *Definice* → *Skupiny* (viz kapitola 18.5).



Obrázek 9.6 Povolení přístupu do Internetu pouze pro vybranou skupinu IP adres

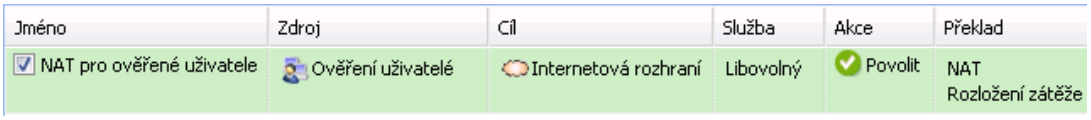
Poznámka:
Definice pravidel tohoto typu je vhodná pouze v případě, že každý uživatel má svůj vlastní počítač (uživatelé se u počítačů nestřídají) a tyto počítače mají přiřazeny statické IP adresy.

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 9.7 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 v *Kerio Control* uživatelský účet. Správce firewallu pak má detailní přehled o tom, kam kteří uživatelé přistupují a jaké služby využívají (anonymní přístup není možný).



Obrázek 9.8 Povolení přístupu do Internetu pouze ověřeným uživatelům

Podrobné informace o přihlašování uživatelů k firewallu naleznete v kapitole 13.1.

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 9.7.

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.

Jméno	Zdroj	Cíl	Služba	Akce	Překlad
Povolit Telnet skupině uživatelů	Telnet povolen	Internetová rozhraní	Telnet	Povolit	NAT Rozložení zátěže
Zakázat Telnet	Libovolný	Internetová rozhraní	Telnet	Zakázat	NAT Rozložení zátěže

Obrázek 9.9 Výjimka — povolení služby Telnet pouze vybrané skupině uživatelů

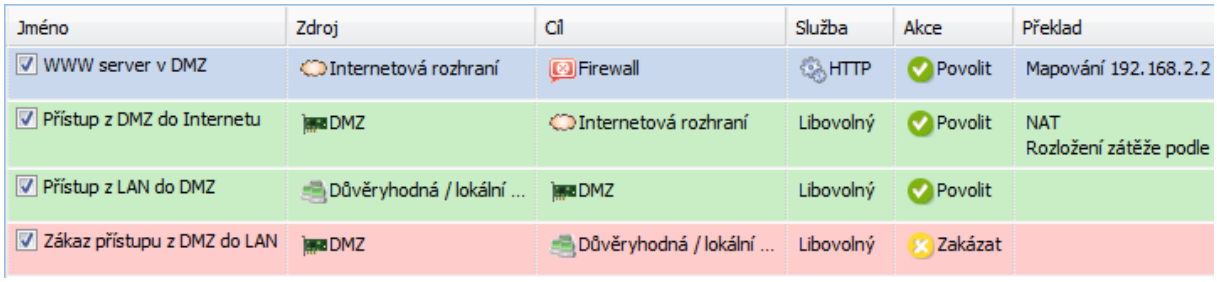
9.5 Demilitarizovaná zóna

Demilitarizovaná zóna (DMZ) je speciální segment lokální sítě vyhrazený pro servery, které jsou zpřístupněné z Internetu. Z tohoto segmentu není povolen přístup do lokální sítě — v případě napadení serveru v demilitarizované zóně nemůže útočník napadnout další servery a počítače v lokální síti.

Jako příklad uvedeme pravidla pro WWW server umístěný v demilitarizované zóně. Demilitarizovaná zóna je připojená k rozhraní *DMZ* zařazeného do skupiny *Ostatní rozhraní* (viz kapitola 7.1). V demilitarizované zóně se používá subsíť `192.168.2.x`, WWW server má IP adresu `192.168.2.2`.

Přidáme následující pravidla:

- Zpřístupnění WWW serveru z Internetu — mapování služby HTTP na serveru v demilitarizované zóně,
- Povolení přístupu z demilitarizované zóny do Internetu prostřednictvím překladu IP adres (NAT) — nutné pro správnou funkčnost mapované služby,
- Povolení přístupu z lokální sítě do demilitarizované zóny — zpřístupnění WWW serveru lokálním uživatelům,
- Zákaz přístupu z demilitarizované zóny do lokální sítě — ochrana proti napadení lokální sítě z DMZ. Toto je obecně zajištěno výchozím pravidlem blokujícím veškerou ostatní komunikaci (blokující pravidlo zde uvádíme pro větší názornost).



Jméno	Zdroj	Cíl	Služba	Akce	Překlad
WWW server v DMZ	Internetová rozhraní	Firewall	HTTP	Povolit	Mapování 192.168.2.2
Přístup z DMZ do Internetu	DMZ	Internetová rozhraní	Libovolný	Povolit	NAT Rozložení zátěže podle
Přístup z LAN do DMZ	Důvěryhodná / lokální ...	DMZ	Libovolný	Povolit	
Zákaz přístupu z DMZ do LAN	DMZ	Důvěryhodná / lokální ...	Libovolný	Zakázat	

Obrázek 9.10 Komunikační pravidla pro demilitarizovanou zónu

Tip
Pro zpřístupnění více serverů v demilitarizované zóně lze s výhodou využít více veřejných IP adres na internetovém rozhraní firewallu — tzv. multihoming (viz kapitola 9.4).

9.6 Policy routing

Pokud je lokální síť připojena do Internetu více linkami s rozložením zátěže (viz kapitola 8.3), 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).

V *Kerio Control* 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.

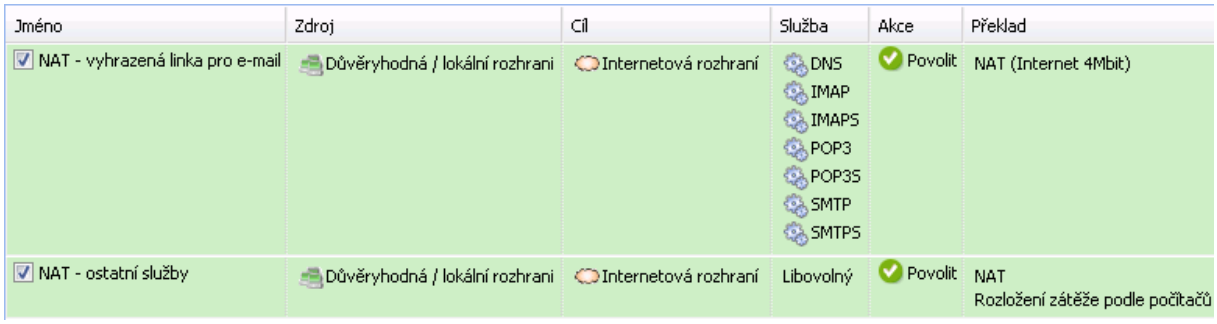
Poznámka:
Komunikační pravidla pro *policy routing* mají vyšší prioritu než cesty definované ve směrovací tabulce (viz kapitola 20.1).

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.

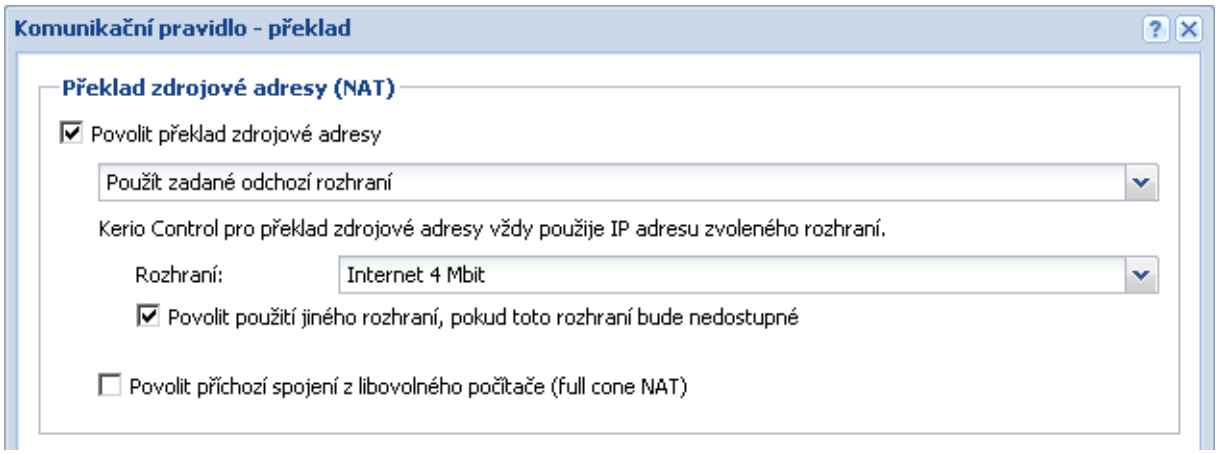
Pro splnění uvedených požadavků definujeme dvě komunikační pravidla:

- 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 9.4).



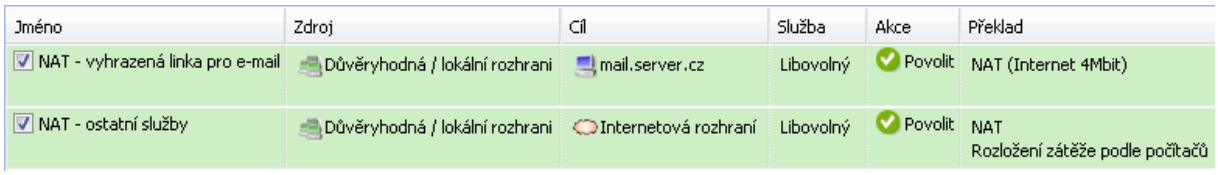
Obrázek 9.11 Policy routing — vyhrazená linka pro e-mail

Nastavení překladu IP adres v pravidle pro e-mailové služby je zřejmé z obrázku 9.12. Doporučujeme povolit použití jiné linky, pokud dojde výpadku vyhrazené linky. V opačném případě by po dobu výpadku vyhrazené linky byly e-mailové služby nedostupné.



Obrázek 9.12 Policy routing — nastavení NAT pro vyhrazenou linku

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 9.13.



Obrázek 9.13 Policy routing — vyhrazená linka pro konkrétní server

Poznámka:
Ve druhém pravidle je použit automatický výběr rozhraní. To znamená, že i linka *Internet 4 Mbit* 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 *Konfigurace* → *Rozhraní* nastavíme této lince rychlost *0 Mbit/s*. Linka pak nebude použita pro automatické rozložení zátěže, ale bude přes ni směrována pouze specifická komunikace dle komunikačních pravidel.

Příklad: Optimalizace rozložení zátěže internetového připojení

Kerio Control nabízí dva způsoby rozložení zátěže internetového připojení: podle zdrojových počítačů (klientů) nebo podle jednotlivých spojení (bližší informace viz kapitola 9.3). 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 9.14. 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	Důvěryhodná / lokální rozhraní	Internetová rozhraní	HTTP HTTPS	Povolit	NAT Rozložení zátěže podle počítačů
NAT - rozložení dle spojení	Důvěryhodná / lokální rozhraní	Internetová rozhraní	Libovolný	Povolit	NAT Rozložení zátěže podle spojení

Obrázek 9.14 Policy routing — optimalizace rozložení zátěže

9.7 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 9.3.

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	Internetová rozhraní	Libovolný	Povolit	NAT Rozložení zátěže podle počítačů

Obrázek 9.15 Komunikační pravidlo povolující přístup do Internetu pouze vybraným uživatelům

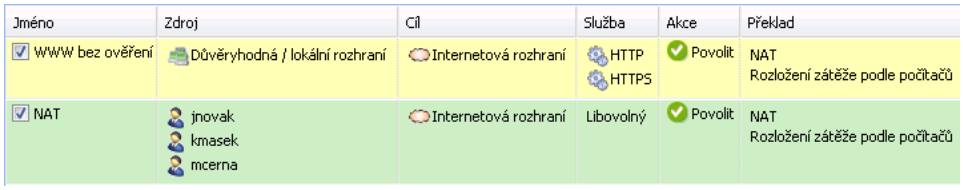
Takto definované pravidlo povolí přístup do Internetu vyjmenovaným uživatelům, pokud budou na firewallu ověřeni. Tito uživatelé však budou muset ručně otevřít přihlašovací stránku WWW rozhraní *Kerio Control* a přihlásit se (podrobnosti viz kapitola 13.1).

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. Toto pravidlo pro překlad adres však nepovolí navázat spojení dříve, než je příslušný uživatel ověřen.

Povolení automatického ověřování

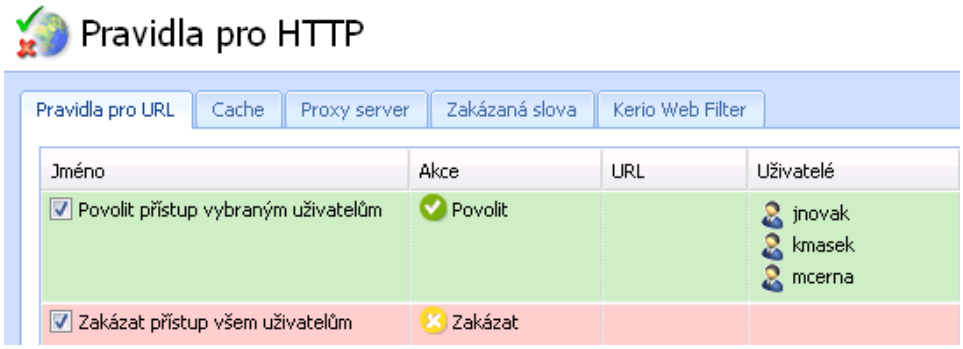
Problém s automatickým ověřováním uživatelů můžeme snadno vyřešit následujícím způsobem:

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



Obrázek 9.16 Komunikační pravidla umožňující automatické přesměrování na přihlašovací stránku

- V pravidlech pro URL (viz kapitola 15.2) povolíme přístup ke všem WWW stránkám vybraným uživatelům a zakážeme přístup všem ostatním uživatelům.



Obrázek 9.17 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 9.16) 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 modul *DNS* v *Kerio Control*, 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*.

9.8 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.

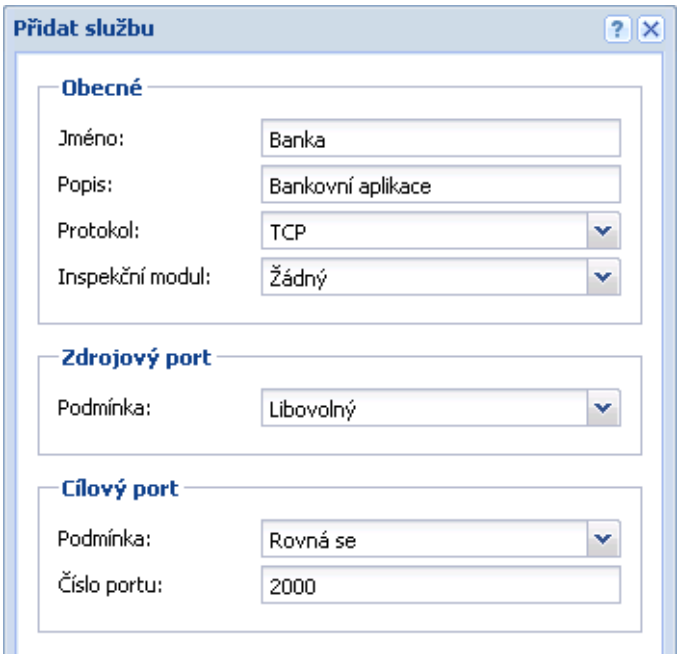
Příklad

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 9.18 Definice služby bez inspekčního modulu

2. V sekci *Konfigurace* → *Zásady komunikace* → *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.

Jméno	Zdroj	Cíl	Služba	Akce	Překlad	Inspekční modul
Bankovní klient	192.168.1.15	server.banka.cz	Banka	Povolit	NAT Rozložení zátěže podle počítačů	Žádný

Obrázek 9.19 Komunikační pravidlo povolující přístup ke službě bez inspekce protokolu

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.

9.9 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 *Kerio Control* 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 9.3.

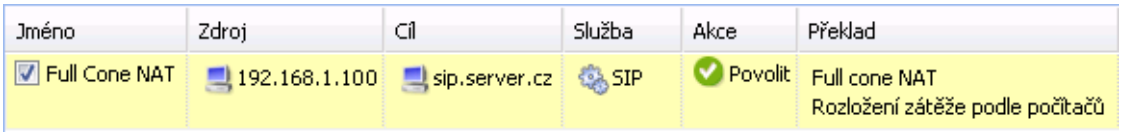
Příklad: SIP telefon v lokální síti

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):



Obrázek 9.20 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 9.3) a zaškrtneme volbu *Povolit příchozí pakety z libovolného počítače (Full cone NAT)*.

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

9.10 Media hairpinning

Kerio Control 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 9.9 (je zřejmé, že do položky *Zdroj* komunikačního pravidla pro *Full cone NAT* dle obrázku 9.20 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. *Kerio Control* 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 9.1) je tato podmínka splněna pravidlem *NAT*.
2. Hairpinning v principu nevyžaduje povolení *Full cone NAT* (viz kapitola 9.9). V uvedeném příkladu je však *Full cone NAT* nutný pro správnou funkci protokolu *SIP*.

Kapitola 10

Firewall a systém prevence útoků

10.1 Systém prevence síťových útoků (IPS)

Kerio Control integruje systém detekce a prevence útoků (IDS/IPS) *Snort*, který chrání firewall a lokální síť před známými typy síťových útoků. V rámci produktu *Kerio Control* se tento systém zjednodušeně nazývá *Prevence útoků* (název v sobě skrývá obě uvedené funkce — prevenci nelze provádět bez detekce).

K čemu slouží a jak funguje systém prevence útoků

Síťový útok je obecně nežádoucí síťová komunikace, která nějakým způsobem narušuje činnost nebo zabezpečení počítače, proti kterému je útok veden, zpravidla za účelem jeho paralýzy, získání neoprávněného přístupu a/nebo odcizení dat. Pro útoky je charakteristické, že se zdánlivě jedná o legitimní síťovou komunikaci a nelze je jednoduše odfiltrovat komunikačními pravidly. Jako příklad uveďme útok typu *DoS* (*Denial of Service* — zablokování služby), kdy útočník navázáním velkého počtu spojení na určitý port způsobí vyčerpání systémových zdrojů serverové aplikace a další klienti se k ní pak již nemohou připojit. Z pohledu firewallu se přitom jedná pouze o přístup na povolený port.

Pro detekci síťových útoků je proto potřeba sofistikovaná analýza síťové komunikace. Systémy detekce síťových útoků obvykle pracují s databázemi známých útoků (podobně jako antivirové programy používají databáze známých virů). Díky pravidelné aktualizaci databáze je zajištěno, že systém bude zachytávat i nové typy útoků.

V současné verzi aplikace *Kerio Control* pracuje systém prevence útoků na všech síťových rozhraních zařazených ve skupině *Internetová rozhraní* (viz kapitola 7). Z toho vyplývá, že detekuje a zachytává síťové útoky přicházející z Internetu, nikoliv z počítačů v lokálních sítích a z VPN klientů (tyto počítače jsou považovány za důvěryhodné).

Pro správnou činnost systému prevence útoku je vyžadováno použití překladu IP adres (NAT — viz kapitola 9.3). Lze jej tedy využít ve všech typických konfiguracích, kdy je *Kerio Control* použit pro ochranu lokální privátní sítě. Je-li *Kerio Control* nasazen jako tzv. neutrální směrovač (bez překladu IP adres), pak nebude systém prevence útoků fungovat správně.

Detekce útoků se provádí před aplikací komunikačních pravidel (viz kapitola 9), aby nedocházelo k ovlivňování detekce nastavenými pravidly.

Konfigurace systému prevence útoků v Kerio Control

Systém prevence útoků lze nastavit v sekci *Konfigurace* → *Zásady komunikace* → *Prevence útoků*.

Detekce známých typů útoků

Kerio Control rozlišuje tři úrovně závažnosti útoků:

- *Velmi závažné* — aktivity, u nichž se s nejvyšší pravděpodobností jedná o skutečné síťové útoky (např. síťová aktivita trojského koně).
- *Středně závažné* — aktivity, které jsou podezřelé a potenciálně škodlivé, ale s určitou pravděpodobností se může jednat o legitimní komunikaci (např. komunikace nestandardním protokolem na standardním portu jiného protokolu).
- *Méně závažné* — podezřelé síťové aktivity, které však nepředstavují bezprostřední hrozbu (např. scannování portů).

Pro každou úroveň závažnosti lze nastavit jednu z těchto akcí:

- *Zaznamenat a zahodit* — informace o detekované aktivitě bude zapsána do záznamu *Security* (viz kapitola 24.11) a příslušná síťová komunikace bude blokována,
- *Zaznamenat* — o detekované aktivitě bude pouze zapsána informace do záznamu *Security*,
- *Žádná akce* — detekovaná aktivita bude ignorována.

Výchozí a doporučené nastavení akcí pro jednotlivé úrovně závažnosti útoků:

- *Velmi závažné* → *Zaznamenat a zahodit*,
- *Středně závažné* → *Zaznamenat*,
- *Méně závažné* → *Žádná akce* (předpokládá se, že by mohlo docházet k velkému množství tzv. falešných poplachů, viz též *Upřesňující nastavení*).

Kliknutím na odkaz lze funkčnost systému prevence útoků otestovat prostřednictvím speciální stránky na serveru společnosti *Kerio Technologies*. Po spuštění testu budou na adresu klienta (tedy veřejnou IP adresu vašeho firewallu) vyslány tři fiktivní útoky vysoké, střední a nízké závažnosti (samozřejmě neškodné). Testovací skript pak vyhodnotí, zda firewall tyto útoky propustil nebo blokoval. V záznamu *Security* se zároveň zobrazí tři odpovídající zprávy — zda firewall jednotlivé útoky blokoval, pouze zaznamenal nebo ignoroval (podrobnosti viz kapitola 24.11).

Poznámka:

Tento test je určen pouze pro systém prevence útoků v produktu *Kerio Control*. Jiné IDS/IPS jím nelze testovat.

Využití databází známých útočníků (černých listin)

Kromě detekce známých typů útoků je možné také detekovat a blokovat síťovou komunikaci z IP adres, které jsou uvedeny v internetových databází známých útočníků (tzv. *blacklists* — černé listiny). V tomto případě se zaznamenává, případně blokuje veškerá komunikace z dané zdrojové IP adresy. Detekce a blokování útočníků tímto způsobem je výrazně rychlejší a méně náročné než detekce jednotlivých typů útoků. Je zde však také několik nevýhod — černé listiny z principu nemohou obsahovat IP

adresy všech potenciálních útočníků, útočníci v mnoha případech zdrojové adresy falšují a na černé listině se také z různých důvodů může objevit IP adresa legitimního klienta nebo serveru. Proto lze pro jednotlivé černé listiny nastavovat stejné akce jako pro detekované útoky:

- *Zaznamenat a zahodit* — informace o detekované komunikaci a blokované IP adrese bude zapsána do záznamu *Security* a z dané IP adresy bude blokována veškerá síťová komunikace,
- *Zaznamenat* — o detekované komunikaci a blokované IP adrese bude pouze zapsána informace do záznamu *Security*,
- *Žádná akce* — detekovaná IP adresa z černé listiny nebude považována za útočníka.

Poznámka:
Kerio Control neumožňuje přidat vlastní databázi (černou listinu).

Aktualizace databází útoků a známých útočníků

Pro správnou činnost systému detekce útoků je potřeba pravidelně aktualizovat databáze známých útoků a IP adres útočníků. *Kerio Control* umožňuje nastavit interval automatické aktualizace (výchozí hodnota je *24 hodin*), případně provést okamžitou aktualizaci dle potřeby (např. po delším výpadku internetového připojení). Za normálních okolností nemá smysl automatické aktualizace vypínat — neaktuální databáze výrazně zhoršují účinnost systému prevence útoků.

> ***Upozornění:***
> Pro aktualizaci databází systému prevence útoků je vyžadovaná platná licence produktu *Kerio Control* nebo registrovaná zkušební verze. Bližší informace viz kapitola 5.

Upřesňující nastavení

Kerio Control umožňuje nastavit některé upřesňující parametry systému prevence útoků. Tyto parametry mohou zvýšit výkon systému prevence útoků a zabránit tzv. falešným poplachům (*false positives*). Důrazně doporučujeme neměnit tyto parametry, pokud si nejste naprosto jisti jejich významem!

Ignorované útoky

V některých případech může být legitimní komunikace detekována jako útok. Pokud se to stává pravidelně, pak je možné pro daný útok definovat výjimku. Definice výjimky spočívá v přidání číselného identifikátoru pravidla do seznamu. Identifikátor pravidla lze zjistit ze záznamu *Security* (viz kapitola 24.11), případně v dokumentaci k systému *Snort* (http://www.snort.org/).

Poznámka:
Výjimky je vhodné definovat pouze v případech, kdy je legitimní komunikace detekována jako útok opakovaně, resp. pravidelně. Není rozumné definovat výjimku při prvním zjištění takovéto události.

Protokolově specifické útoky

Některé útoky mohou být zaměřeny na bezpečnostní chyby v konkrétních aplikačních protokolech. Proto je za normálních okolností zbytečné detekovat tyto útoky v komunikaci jiných aplikačních protokolů. Pro jednotlivé protokoly, které systém detekce útoků rozeznává, jsou předdefinovány seznamy standardních portů, případně často používaných portů. Seznamy mohou obsahovat jednotlivá čísla portů oddělená čárkami, případně rozsahy portů (počáteční a koncový port oddělené pomlčkou bez mezer).

Pokud je z Internetu zpřístupněná aplikace, která používá některý z uvedených protokolů na nestandardním portu (např. *HTTP* na portu *10000*), pak je vhodné přidat tento port do seznamu portů, na kterých budou detekovány útoky specifické pro protokol *HTTP*.

Je-li naopak na některém uvedeném portu provozována aplikace používající jiný protokol (např. VPN server na portu *8000*), pak je doporučeno tento port odebrat ze seznamu portů pro daný protokol — na tomto portu je zbytečné detekci provádět, detekce zbytečně zatěžuje firewall a mohlo by také docházet k falešným poplachům.

10.2 Filtrování MAC adres

Kromě *Komunikačních pravidel*, která filtrují síťovou komunikaci na základě IP adres, protokolů a portů (viz kapitola 9), umožňuje *Kerio Control* také „nízkoúrovňové“ filtrování na základě hardwarových adres (tzv. MAC adres) jednotlivých počítačů a síťových zařízení. Filtrováním fyzických adres lze např. zabránit uživatelům svévolně připojovat vlastní zařízení do sítě nebo obejít pravidla firewallu změnou IP adresy svého počítače.

Poznámka:
Filtr MAC adres pracuje na nižší úrovni než komunikační pravidla firewallu (viz kapitola 9), a proto je aplikován dříve než komunikační pravidla.

Filtrování MAC adres lze nastavit v sekci *Konfigurace* → *Zásady komunikace* → *Bezpečnostní volby*.

Síťová rozhraní

Filtr MAC adres může být aplikován na libovolném síťovém rozhraní firewallu, které je typu *Ethernet* nebo *Wi-Fi*. Doporučujeme však důkladně zvážit, čeho chcete docílit, a vybrat pouze ta rozhraní, na kterých má být síťová komunikace filtrována. Chcete-li např. blokovat nežádoucí zařízení v lokální síti, nemá smysl zapínat filtrování MAC adres na internetových rozhraních. Tím je pouze zbytečně zatěžován firewall, a může také dojít k blokování internetové komunikace.

Režim filtrování

Filtr MAC adres může pracovat v jednom ze dvou režimů:

- Blokování počítačů s uvedenými MAC adresami.
  Filtr bude blokovat pouze komunikaci počítačů (zařízení) s MAC adresami uvedenými na seznamu. Komunikace všech ostatních počítačů bude povolena. Tento režim lze využít k rychlému zablokování určitých MAC adres, nezabrání však připojení nových, dosud neznámých zařízení. Další nevýhodou je

skutečnost, že řada systémů a zařízení umožňuje MAC adresu síťového adaptéru změnit.

- Povolení komunikace počítačů s uvedenými MAC adresami.
  Filtr povolí pouze komunikaci počítačů s MAC adresami uvedenými na seznamu, komunikace všech ostatních počítačů bude blokována. Tento režim filtrování je velmi účinný, jsou blokovány všechny neznámé MAC adresy (v jedné fyzické síti nemohou být dvě zařízení se shodnou MAC adresou — zneužití povolené MAC adresy je proto velmi obtížné nebo dokonce nemožné).
  Při použití tohoto režimu je však nutné vytvořit a udržovat kompletní seznam MAC adres všech zařízení, jejichž komunikace má být povolena. U větších sítí to může být poměrně náročný úkol.

Seznam MAC adres

Tento seznam obsahuje MAC adresy počítačů, jejichž komunikace bude filtrována nebo naopak povolena — v závislosti na zvoleném režimu.
MAC adresy se zadávají jako šestice bytů (hexadecimálních čísel) oddělených dvojtečkami (např.: `a0:de:bf:33:ce:12`) nebo pomlčkami (např.: `a0-de-bf-33-ce-12`), případně ve zhuštěném tvaru bez oddělovačů (např.: `a0debf33ce12`).
Každá MAC adresa může být volitelně doplněna popisem pro snazší orientaci, jakému počítači (zařízení) daná adresa patří. Doporučujeme tyto popisy důsledně vyplňovat — samotná MAC adresa nemá prakticky žádnou vypovídací hodnotu.

10.3 Volby pro zvýšení bezpečnosti

Kerio Control nabízí několik doplňkových možností filtrování komunikace, které nelze definovat komunikačními pravidly. Tyto volby lze aktivovat a nastavit v sekci *Konfigurace* → *Zásady komunikace* → *Bezpečnostní volby*, záložka *Různé*.

Kontrola zdrojových adres (Anti-Spoofing)

Anti-Spoofing je kontrola, zda na jednotlivá rozhraní počítače s *Kerio Control* přicházejí pouze pakety s přípustnými zdrojovými IP adresami. Tato funkce chrání počítač s *Kerio Control* 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 *Kerio Control* 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 24.11).

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, *Kerio Control* nepovolí otevřít další spojení v daném směru.

Uvedená omezení chrání firewall (počítač s *Kerio Control*) 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).

Filtrování komunikace protokolem IPv6

Kerio Control umožňuje blokovat komunikaci protokolem IPv6. V novějších operačních systémech (např. *Windows Vista* a *Windows 7*) je tento protokol implicitně povolen a počítač má přidělenou automaticky generovanou IPv6 adresu. To může představovat značné bezpečnostní riziko.

Kerio Control umožňuje blokovat:

- *Nativní komunikaci IPv6* — Kerio Control přímo připojen do sítě, kde je podporován protokol IPv6, ale nechcete jej používat.

  Tato možnost je dostupná pouze v edici pro systém Windows a ve výchozím stavu je zapnutá.

  V edicích *Software Appliance* a *Box* je veškerá nativní IPv6 komunikace implicitně povolena (protokol IPv6 lze povolit nebo zakázat na jednotlivých síťových rozhraních).

- *Tunelovanou komunikaci IPv6* — pro usnadnění přechodu na IPv6 bylo vyvinuto několik protokolů, které umožňují zapouzdřit pakety IPv6 do IPv4 a komunikovat tak tímto protokolem přes sítě, které dosud podporují pouze IPv4.

  Z bezpečnostních důvodů je ve výchozím nastavení tunelovaná komunikace IPv6 blokována.

V případě blokování tunelované komunikace IPv6 mohou být uděleny výjimky — tunelovaná komunikace počítačů s konkrétními adresami IPv4 nebude blokována. Výjimky se definují výběrem skupiny IPv4 adres (viz kapitola 17.1). Skupina může obsahovat IPv4 adresy počítačů v lokální síti i v Internetu.

10.4 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).

Kerio Control 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[5]. *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 veškeré komunikace* — příslušnému počítači bude zcela zablokován přístup do Internetu,
- *Povolení pouze „bezpečné“ komunikace* — příslušnému počítači bude povolena pouze komunikace, která bezpečně nepatří do P2P sítí (např. WWW, e-mail atd.).

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) nebo povolit pouze služby, které bezpečně nepatří do P2P sítí. Nastavené omezení bude vždy aplikováno na všechny klienty *P2P* sítí, které *P2P Eliminator* detekuje.

[5] Důkladné testy však prokázaly, že úspěšnost této detekce je velmi vysoká.

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 18.1). 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 správce firewallu. Doba blokování komunikace by měla být dostatečně dlouhá, aby si uživatel uvědomil následky své činnosti a nepokoušel se znovu připojovat k *P2P* sítím.

Poznámka:

1. Je-li z určitého počítače k firewallu přihlášen uživatel, který má právo používat *P2P* sítě (viz kapitola 18.1), 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 21.2).
3. Chceme-li při detekci *P2P* zasílat e-mail jiné osobě (např. správci firewallu), můžeme definovat příslušnou výstrahu v sekci *Konfigurace* → *Statistiky a výstrahy*, záložka *Nastavení výstrah*. Podrobnosti viz kapitola 21.5.

Parametry pro detekci P2P sítí

Tlačítko *Upřesnění* otevírá dialog pro nastavení 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 17.3).

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).

Kapitola 11

Síťové služby a konfigurace lokální sítě

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

- Modul *DNS* — slouží jako jednoduchý DNS server pro lokální síť,
- *DHCP server* — zajišťuje automatickou konfiguraci protokolu IPv4 na počítačích v lokální síti,
- *Ohlašování směrovače IPv6* — zajišťuje automatickou bezestavovou konfiguraci protokolu IPv6 na počítačích v lokální síti,
- *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),
- Klient služby *DDNS* — zajišťuje automatickou aktualizaci záznamů pro firewall ve veřejném dynamickém DNS.

11.1 Modul DNS

Modul *DNS* slouží v *Kerio Control* ke zjednodušení konfigurace DNS na počítačích v lokální síti a pro zrychlení odpovědí na opakované DNS dotazy.

Modul DNS pracuje pouze nad protokolem IPv4. Protokol IPv6 není podporován.

Na počítačích v lokální síti lze obecně nastavit DNS 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* v *Kerio Control*. 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, předá jej některému z DNS serverů nastavených na internetové lince, přes kterou je dotaz odesílán. Podrobnosti o konfiguraci síťových rozhraní firewallu naleznete v kapitole 7, bližší informace o možnostech internetového připojení v kapitole 8.

Konfigurace modulu DNS

Ve výchozím nastavení *Kerio Control* 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*.

Povolit službu DNS forwarder

Tato volba zapíná / vypíná DNS server v *Kerio Control*. 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 *Kerio Control*.

> ***Upozornění:***
> Pokud ve vaší síťové konfiguraci nepoužijete modul DNS, 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 27.3). Díky tomu zůstávají záznamy v DNS cache uchovány i při zastavení *Kerio Control 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 v *Kerio Control* (viz kapitola 11.5).

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 11.2) bude odpověď obsahovat vždy aktuální IP adresu.

Poznámka:
Modul *DNS* v *Kerio Control* nedokáže zodpovídat tzv. reverzní DNS dotazy (tzn. zjištění jména počítače z IP adresy). Tyto dotazy jsou vždy předávány na jiný DNS server.

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.

- *Tabulka jmen počítačů* — tabulka, definovaná správcem *Kerio Control*. Každý řádek této tabulky obsahuje IP adresu počítače a seznam odpovídajících DNS jmen.
- *Tabulka adres přidělených DHCP serverem* — jsou-li počítače v lokální síti konfigurovány pomocí DHCP serveru v *Kerio Control* (viz kapitola 11.2), 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* může z databáze DHCP serveru zjistit, jaká IP adresa je v tomto okamžiku přidělena danému jménu počítače. Na dotaz na dané jméno počítače v lokální síti tedy vždy odpoví správnou (aktuální) IP adresou. Tímto způsobem dochází de facto k dynamické aktualizaci DNS.

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

Lokální DNS doména

Do pole *Při prohledávání tabulky jmen počítačů 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 tabulce jmen počítačů uvedena lokální jména počítačů 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.

Tabulka jmen počítačů

Tabulka jmen počítačů je seznam IP adres a k nim příslušných DNS jmen počítačů. Na základě této tabulky dokáže *Kerio Control* zjistit IP adresu lokálního počítače zadaného jménem.

Každý řádek tabulky je záznam pro jednu IP adresu. DNS jména mohou být uvedena bez domény nebo včetně domény — při vyhledávání se provádí výše popsaná kombinace s lokální doménou.

Jedné IP adrese může být přiřazeno více DNS jmen. Toto lze definovat dvěma způsoby:

- Zapsat vše do jednoho záznamu a jednotlivá jména oddělit středníky. Příklad:

  ```
  192.168.1.10 server;mail
  ```

  Výhodou je úsporný zápis. První uvedené jméno je vždy považováno za primární (tzv. kanonické jméno), ostatní jsou jeho aliasy.

- Vytvořit pro každé jméno samostatný záznam. Příklad:

  ```
  192.168.1.10 server
  ```

  ```
  192.168.1.10 mail
  ```

  V tomto případě je možné nastavit primární jméno dle potřeby. Záznamy se přesouvají šipkovými tlačítky na pravé straně okna. Jméno, které je pro danou IP adresu v seznamu uvedeno jako první, bude považováno za primární (kanonické).

Doporučujeme vybrat si jeden z uvedených způsobů zápisu. Při kombinaci obou způsobů bude tabulka jmen počítačů nepřehledná.

Jednomu DNS jménu může být přiřazeno více IP adres (např. počítač s více síťovými adaptéry). V tomto případě je potřeba do tabulky přidat záznam pro každou IP adresu, přičemž DNS jméno bude ve všech těchto záznamech stejné.

Upozornění:
Obsah tabulky jmen počítačů se ukládá do systémového souboru `hosts`. Proto nedoporučujeme na serveru *Kerio Control* upravovat tento soubor ručně!

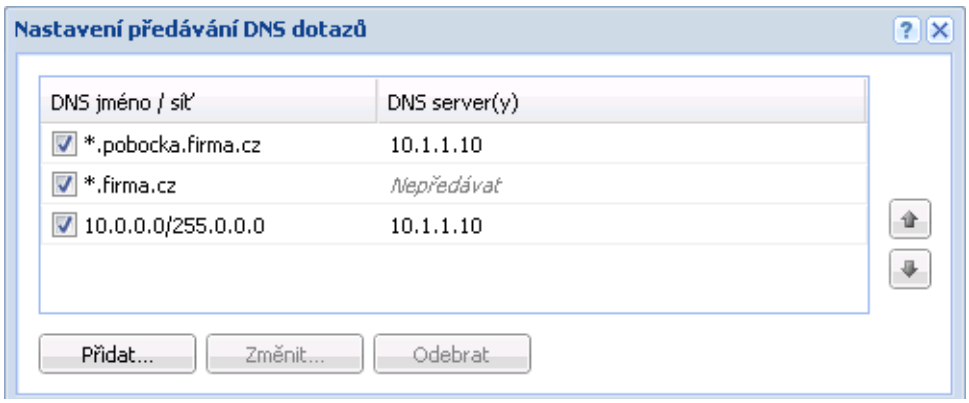
Nastavení předávání DNS dotazů

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 25).

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 výše), pak se pravidla pro předávání dotazů uplatní pouze v případě, že modul *DNS* nedokáže dotaz zodpovědět na základě informací z tabulky jmen počítačů a/nebo tabulky přidělených adres DHCP serveru.

Tlačítko *Definovat* v konfiguraci modulu *DNS* otevírá dialog pro nastavení pravidel pro předávání DNS dotazů.



Obrázek 11.1 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.

Definice pravidla:

- Pravidlo pro *DNS dotaz na jméno* — 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 — *Kerio Control* bude pouze prohledávat lokální tabulku jmen počítačů a/nebo

tabulku DHCP serveru (viz dále). Pokud zde dotazované jméno, resp. IP adresu nenalezne, odpoví klientovi, že toto jméno/adresa neexistuje.

Poznámka:
Volba *Nepředávat* nemá smysl pro reverzní DNS dotazy, protože ty nedokáže modul *DNS* v *Kerio Control* sám zodpovědět.

11.2 DHCP server

Protokol DHCP 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.).

Kerio Control navíc umožňuje automatickou konfiguraci samotného DHCP serveru, což znamená, že se automaticky vytvářejí a aktualizují rozsahy IP adres a přidělované parametry podle síťových rozhraní zařazených ve skupině *Důvěryhodná / Lokální rozhraní* (viz kapitola 7). DHCP server tedy stačí de facto pouze zapnout. Pokud automatická konfigurace z nějakého důvodu nevyhovuje, pak se lze jednoduše přepnout do režimu ruční konfigurace.

Konfigurace DHCP serveru

K nastavení DHCP serveru v *Kerio Control* slouží sekce *Konfigurace* → *Konfigurace LAN* → *DHCP server*. Zde lze definovat rozsahy IP adres, rezervace, volitelné parametry a zobrazovat informace o přidělených adresách a statistiky DHCP serveru. Konfiguraci je možné provádět i v případě, že je DHCP server vypnut.

Automatická konfigurace rozsahů IP adres

Ve výchozím nastavení pracuje DHCP server v režimu automatické konfigurace rozsahů IP adres. V tomto režimu *Kerio Control* načítá parametry síťových rozhraní zařazených ve skupině *Důvěryhodná / Lokální rozhraní* a na základě těchto parametrů automaticky vytváří a aktualizuje rozsahy IP adres pro příslušné subsítě. Při změně rozhraní ve skupině *Důvěryhodná / Lokální rozhraní* tedy bude automaticky aktualizována konfigurace DHCP serveru.

Pro subsíť každého rozhraní bude vytvořen rozsah s následujícími parametry:

- *Rozsah adres* — dle IP adresy příslušného rozhraní a odpovídající masky subsítě.

  Rozsah se vytváří tak, aby pokryl danou subsíť s určitou rezervou pro staticky přidělené adresy (např. při použití masky `255.255.255.0` bude vytvořen rozsah adres `x.x.x.11` až `x.x.x.254`). Pokud adresa rozhraní patří do vytvořeného rozsahu, pak je pro ni automaticky definována výjimka.

- *Maska subsítě* — dle příslušného rozhraní.

- *Výchozí brána* — IP adresa příslušného rozhraní.

- *DNS server* — IP adresa příslušného rozhraní.

Případně mohou být nastaveny další parametry, které lze z nastavení daného rozhraní načíst (DNS doména, adresa WINS serveru). Zde již záleží na operačním systému firewallu a konkrétní konfiguraci daného rozhraní.

Ruční definice rozsahů IP adres

Nechcete-li využít automatickou konfiguraci rozsahů IP adres, můžete se přepnout do režimu ruční konfigurace. Mějte však na paměti, že při případné změně rozhraní ve skupině *Důvěryhodná / Lokální rozhraní* (např. přidání nového rozhraní, změna IP adresy atd.) je nutné ručně aktualizovat rozsahy adres definované v DHCP serveru!

V každé IP subsíti je možné definovat pouze jeden rozsah adres.

Poznámka:
V rozhraní *Kerio Control Administration* je rovněž možné použít šablonu rozsahu, ve které jsou již předvyplněny parametry rozsahu na podle příslušného rozhraní firewallu. Bližší informace viz výše (sekce *Automatická konfigurace rozsahů IP adres*).

Definice rozsahu IP adres:

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

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:
Administrační rozhraní 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, pak je po jejím uplynutí tato adresa automaticky uvolněna a může být přidělena jinému klientovi.

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

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

Příklad
V subsíti `192.168.1.0` chceme vytvořit dva rozsahy adres: `192.168.1.10` až `192.168.1.49` a `192.168.1.61` až `192.168.1.100`. Adresy `192.168.1.50` až `192.168.1.60` mají zůstat vyhrazeny pro jiné účely.
Vytvoříme rozsah adres `192.168.1.10` až `192.168.1.100` a stisknutím tlačítka *Výjimky* definujeme rozsah adres `192.168.1.50` až `192.168.1.60`, které nemají být DHCP serverem přidělovány.

Parametry DHCP
Dialog *Rozsah IP adres* umožňuje zadání DHCP parametrů, které budou přidělovány společně s IP adresou. Pro správnou funkci TCP/IP na klientských stanicích je potřeba přidělit tyto parametry:

- *003: Default gateway* (výchozí brána) — IP adresa směrovače, který je výchozí branou pro danou subsíť (tzn. IP adresa rozhraní firewallu, ke kterému je tato subsíť připojena). Výchozí brána v jiné subsíti nemá žádný smysl — byla by pro klienty nedosažitelná.
- *006: 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 IP adresu počítače s *Kerio Control*. Modul *DNS* totiž dokáže spolupracovat s DHCP serverem (viz kapitola 11.1) a na dotazy na jména lokálních počítačů bude vždy odpovídat správnou IP adresou.

Protokol DHCP dále umožňuje přidělovat řadu volitelných parametrů, např.:

- *015: Domain name* — lokální internetová doména (neslouží k zadání jména domény *Windows NT*).
- *066: TFTP server name* — jméno nebo IP adresa TFTP serveru. Protokol TFTP využívá např. Kerio Operator pro automatickou konfiguraci telefonů.

Přidělené adresy a rezervace

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

Poznámka:
Ikona s písmenem R označuje IP adresy, které jsou rezervovány.

Sloupce okna *Přidělené IP adresy* zobrazují následující informace:

- *IP adresa* — přidělená IP adresa,
- *Jméno* — název / popis rezervace (u dynamicky přidělených adres je prázdné),
- *Výrobce* — výrobce síťového adaptéru klienta (zjištěný z MAC adresy),
- *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:
  Informace o expirovaných a uvolněných IP adresách DHCP server udržuje pro případ, kdy příslušný klient opět požádá o přidělení IP adresy — DHCP server se snaží přidělovat jednomu klientovi stále tutéž adresu. V případě nedostatku volných IP adres však mohou být tyto adresy přiděleny jiným klientům.
- *Uživatel* — jméno uživatele, který je z daného počítače přihlášen k firewallu.
- *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*.

Tlačítkem *Odebrat* lze okamžitě uvolnit vybranou IP adresu a/nebo zrušit rezervaci IP adresy. Příslušnému klientovi bude vyslána řídicí zpráva *DHCPRELEASE*.

Rezervace IP adresy

DHCP server umožňuje vyhradit (rezervovat) vybranou IP adresu pro konkrétní počítač. Rezervaci lze provést obou režimech konfigurace rozsahů IP adres (ručním i automatickém). Samotným přidáním rezervace v automatickém režimu nedochází k přepnutí do ručního režimu.

Tlačítkem *Přidat* je možné:

- Vytvořit novou rezervaci na základě zadaných parametrů.
- Rezervovat dynamicky přidělenou IP adresu.

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*).

Při přidělení rezervované IP adresy budou automaticky použity DHCP parametry nastavení v příslušném rozsahu. V dialogu *Rezervace adresy* je možné přidat další parametry, případně nastavit specifické hodnoty již existujících parametrů.

Poznámka:
Při rezervaci dynamicky přidělené adresy je možné IP adresu i změnit. De facto vytváříme novou rezervaci, ale není nutné ručně zadávat MAC adresu.

11.3 Ohlašování směrovače IPv6

Ohlašování směrovače IPv6 slouží pro automatickou bezestavovou konfiguraci IPv6 zařízení v lokální síti (SLAAC). Přidejte záznam pro každou síť, ve které se má Kerio Control ohlašovat jako výchozí směrovač.

Nastavení se provádí v sekci *Konfigurace* → *Konfigurace LAN* → *Ohlašování směrovače IPv6*. Záznam ohlašování směrovače má tyto parametry:

- *Rozhraní* — rozhraní připojené k síti, do níž se má směrovač ohlašovat.
- *Prefix* — prefix IPv6 adresy (adresa podsítě). Zapisuje se ve tvaru IPv6 adresy a musí odpovídat zadané délce prefixu, tzn. všechny bity vyšší než délka prefixu musí být nulové.
- *Délka prefixu* — určuje počet bitů IPv6 adresy, které se považují za prefix (adresu podsítě).

11.4 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 *Kerio Control* a při dalším přístupu nemusejí být znovu stahovány z WWW serveru.

Poznámka:
Na zařízení *Kerio Control Box* není HTTP cache z technických důvodů k dispozici.

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 *Kerio Control* je tato podmínka splněna pro protokol HTTP na standardním portu 80 (podrobnosti viz kapitoly 9.3 a 17.3).

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

Povolit cache pro přímý přístup na WWW stránky
Zapnutí cache pro HTTP komunikaci obsluhovanou inspekčním modulem HTTP (tj. přímý přístup do Internetu).

Povolit cache pro netransparentní proxy server v Kerio Control

Zapnutí cache pro HTTP komunikaci přes proxy server v *Kerio Control* (viz kapitola 11.5).

TTL pro protokol HTTP

Výchozí doba uchování objektů v cache (standardně jeden den). Platí pro všechny objekty, pro které není nastavená specifická doba uchování v cache.

Specifická nastavení pro URL

Pro objekty na konkrétních serverech nebo stránkách je možné nastavit jinou (zpravidla kratší) dobu uchování v cache.

Do pravidla zadejte URL nebo část URL objektů, pro které bude pravidlo platit. Doba uchování objektu cache se zadává v hodinách. Hodnota 0 znamená, že objekt nebude uložen do cache.

Velikost cache

Velikost souboru cache na disku.

Maximální velikost cache je omezena na *2 GB* (*2047 MB*). Praktické testy však ukazují, že při velikosti cache větší než *1 GB* (*1024 MB*) výrazně klesá rychlost vyhledávání objektů a tím i účinnost cache jako takové. Proto nedoporučujeme vytvářet cache větší než *1 GB*.

Cache je fyzicky umístěna v podadresáři `cache` „hlavního“ adresáře aplikace *Kerio Control*, tj.:

- v edici pro systém *Windows* typicky:

  `C:\Program Files\Kerio\WinRoute\Firewall\cache`

- v edici *Appliance* vždy:

  `/opt/kerio/winroute/cache`

Na příslušném disku musí být dostatek volného místa, v krajním případě je potřeba nastavit velikost cache s ohledem na zbývající volné místo na disku. 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).

Při nastavení velikosti cache větší než je aktuální volné místo na příslušném disku se cache neinicializuje a do záznamu *Error* (viz kapitola 24.8) se zapíše odpovídající chybové hlášení.

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).

Sledování stavu a správa cache

Kerio Control umožňuje sledovat využití HTTP cache a v případě potřeby vymazat obsah cache.

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 *Kerio Control 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.

Tlačítko *Vyprázdnit cache* jednorázově vymaže všechny objekty uložené v cache.

11.5 Proxy server

Kerio Control 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 *Kerio Control* není možné přímé připojení, je třeba použít proxy server poskytovatele Internetu.

   Proxy server v *Kerio Control* 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 15.2). 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 *Kerio Control* 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. *Kerio Control* 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 v *Kerio Control* 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 v *Kerio Control* naleznete v kapitole 27.5.

Konfigurace proxy serveru

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

Povolit netransparentní proxy server

Tato volba zapíná HTTP proxy server v *Kerio Control* 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 Kerio Control* tento port sice akceptuje, ale proxy server na něm nespustí a do záznamu *Error* (viz kapitola 24.8) 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 tunelovaná 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 zabezpečeným HTTPS spojením.
Je-li tato volba vypnuta, pak proxy server povoluje navázání HTTPS 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 v *Kerio Control* obsluhována inspekčními moduly, které propustí pouze platné HTTP a FTP požadavky.

Předávat požadavky nadřazenému...

Zapnutím této volby bude proxy server ve *Kerio Control* 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 *Kerio Control* do Internetu (pro kontrolu a stahování nových verzí, aktualizaci integrovaného antiviru *Sophos* a přístup do online databází modulu *Kerio Control 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*, *Google Chrome* apod.) umožňuje automatickou konfiguraci skriptem staženým ze zadaného URL.

V případě proxy serveru v *Kerio Control* 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 *Kerio Control* 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 *Kerio Control* a lokální sítě:

- *Přímý přístup* — v prohlížeči nebude nastaven žádný proxy server.
- *Netransparentní proxy server v Kerio Control* — v prohlížeči bude nastavena IP adresa počítače s *Kerio Control* 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 v *Kerio Control* (viz kapitola 11.2). 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.

11.6 Dynamický DNS pro veřejnou IP adresu firewallu

Kerio Control poskytuje (mimo jiné) služby pro vzdálený přístup do lokální sítě z Internetu (*VPN server* — viz kapitola 25 a rozhraní *Clientless SSL-VPN* — viz kapitola 26). Z Internetu mohou být přístupné i další služby — např. webové rozhraní *Kerio Control* (viz kapitola 14), správa *Kerio Control* (viz kapitola 4) nebo libovolná jiná služba (např. WWW server v lokální síti — viz kapitola 9.4). 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 v *Kerio Control*. 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 *Kerio Control*.

Je-li *Kerio Control* nastaven pro spolupráci s dynamickým DNS, pak při každé změně IP adresy internetového rozhraní (včetně přepnutí primárního / záložního internetového připojení — viz kapitola 8.4) 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 v Kerio Control

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

Jak již bylo zmíněno, nejprve je potřeba si zřídit účet (tzn. požadovaný dynamický DNS záznam s příslušnými přístupovými právy) u některého poskytovatele služby DDNS. *Kerio Control* 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*.

Kapitola 12

Řízení šířky pásma a QoS

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.

Přenosová rychlost (propustnost, kapacita) internetové linky se označuje termínem *šířka pásma*. Kerio Control obsahuje modul *Řízení šířky pásma*, který umožňuje optimalizovat využití internetového připojení, aby nedošlo k jeho zahlcení a byla zajištěna funkčnost důležitých síťových služeb.

12.1 Jak funguje řízení šířky pásma?

Modul *Řízení šířky pásma* má dvě základní funkce:

Omezení rychlosti datových přenosů
: Tato funkce slouží především pro omezení neproduktivní komunikace, která zbytečně zatěžuje linku na úkor jiných služeb (stahování velkých objemů dat, prohlížení videa apod.).

Vyhrazení pásma pro určité služby
: Služby, které jsou důležité pro chod organizace (e-mail, IP telefonie atd.), mohou mít vyhrazenou určitou část pásma internetové linky. Toto pásmo je vždy k dispozici, bez ohledu na aktuální zatížení linky. Uživatelé tak žádnou svou aktivitou nemohou ohrozit důležité síťové služby a chod organizace. Rezervace pásma pro určitou službu se označuje zkratkou *QoS* (*Quality of Service* — zajištění kvality služby).

12.2 Rychlosti internetových linek

Pro správnou funkci řízení šířky pásma je potřeba správně stanovit rychlost linky, resp. linek použitých pro internetové připojení (v dolní části stránky).

Rychlost linky lze nastavit v libovolných jednotkách, není třeba nic přepočítávat. Malé *b* znamená bity, velké *B* bajty (*1B = 8b*).

Čím přesněji bude rychlost linky nastavena, tím lépe bude řízení šířky pásma fungovat. Skutečná rychlost linky je typicky 80% rychlosti udávané poskytovatelem internetového připojení.

Příklad: Pro ASDL linku s deklarovanými parametry *8192/512 kbit/s* nastavíme rychlost v příchozím směru (download) *6 Mbit/s* a rychlost v odchozím směru (upload) *400 Kbit/s*.

12.3 Pravidla pro řízení šířky pásma

Řízení šířky pásma se definuje posloupností pravidel. Každé pravidlo popisuje určitý typ komunikace a stanovuje omezení a/nebo rezervaci pásma internetového připojení pro tuto komunikaci.

Typ komunikace

Komunikaci, pro kterou chceme omezovat nebo rezervovat pásmo, lze popsat jako:

- Předdefinovaný typ komunikace — WWW, e-mail, FTP, multimédia atd.,
- Komunikace vybraných uživatelů,
- Komunikace všech uživatelů, kteří překročili některou z kvót přenesených dat,
- Přenosy velkých objemů dat,
- Pakety vyhovující vybranému komunikačnímu pravidlu (viz kapitola 9),
- Komunikace odpovídající pravidlu pro URL (viz kapitola 15.2) nebo pravidlu pro FTP (viz kapitola 15.5),
- Komunikace vybrané síťové služby (viz kapitola 17.3),
- Pakety s určitou hodnotou *DSCP*.
  Hodnotu *DSCP* lze v *Kerio Control* nastavit pomocí komunikačních pravidel, může však být nastavena i jinými směrovači na trase, případně klientem a/nebo serverem.

Download, Upload

V každém směru komunikace můžeme omezit maximální přenosovou rychlost nebo naopak rezervovat určitou minimální šířku pásma. Kombinací obou akcí lze zajistit, aby ani služba, pro kterou je pásmo rezervováno, neubírala příliš vekou část pásma ostatním službám.

Rozhraní

V některých případech však může být žádoucí definovat různá pravidla pro jednotlivá rozhraní / linky. Např. v případě zálohovaného internetového připojení nemusí být komunikace na rychlé primární lince nijak omezována, ale na pomalé záložní lince je potřeba definovat omezení, aby nedošlo k jejímu zahlcení.

Pravidlo pro řízení šířky pásma může platit pro všechna internetová rozhraní, nebo pro jedno konkrétní rozhraní. Chceme-li definovat omezení na více rozhraních (ale ne na všech), je potřeba přidat samostatné pravidlo pro každé rozhraní.

Časová platnost

Každé pravidlo pro řízení šířky pásma může mít omezenou časovou platnost — typicky nastavení přísnějších omezení v pracovní době. Časové intervaly (viz kapitola 17.2) umožňují definovat prakticky libovolnou časovou podmínku.

Graf internetové komunikace

Časový průběh komunikace odpovídající pravidlu můžeme sledovat v sekci *Stav* → *Grafy síťové komunikace* (nejvýše za poslední den). Graf ukáže, jak daná komunikace skutečně zatěžuje internetovou linku a pomáhá optimalizovat pravidla pro řízení šířky pásma (např. můžeme zjistit, že jsme pro určitou službu definovali zbytečně velkou část pásma). Lokální komunikace se nezaznamenává.

12.4 Jak funguje detekce spojení přenášejících velký objem dat?

V této kapitole uvádíme popis způsobu, jakým modul *Řízení šířky pásma* detekuje spojení přenášející velké objemy dat. Tento popis slouží pouze jako doplňující informace — pro konfiguraci řízení 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.

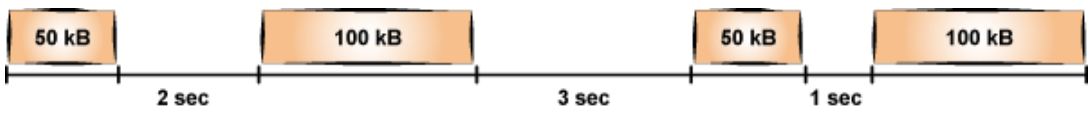
Je-li zaznamenána prodleva delší než stanovená hodnota, pak se vynuluje čítač objemu přenesených dat a počínaje dalším blokem dat probíhá další vyhodnocování výše popsaným způsobem. Z toho vyplývá, že za přenos velkého objemu dat je považováno každé takové spojení, které *kdykoliv* vykáže uvedené charakteristiky.

Parametry detekce jsou následující: spojením musí být přeneseno alespoň *200 KB* dat, aniž by nastala prodleva alespoň *5 sec*. Tyto hodnoty byly stanoveny optimálně na základě dlouhodobého testování a nelze je měnit.

Příklady

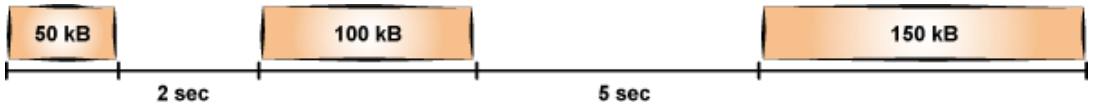
Pro snazší pochopení principu detekce spojení přenášejících velký objem dat uvádíme několik typických příkladů.

1. Spojení na obrázku 12.1 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.



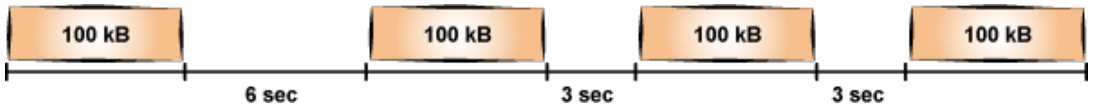
Obrázek 12.1 Příklad spojení — krátké prodlevy

2. Spojení na obrázku 12.2 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 12.2 Příklad spojení — dlouhá prodleva

3. Spojením na obrázku 12.3 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 12.3 Příklad spojení — dlouhá prodleva na začátku

Kapitola 13

Ověřování uživatelů

Kerio Control 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 (viz kapitola 23), v záznamech (viz kapitola 24), přehledu otevřených spojení (viz kapitola 21.3) a přehledu počítačů a uživatelů (viz kapitola 21.2). 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*.

13.1 Ověřování uživatelů na firewallu

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

- Ručně — ve svém prohlížeči otevře WWW rozhraní *Kerio Control*

  `https://server:4081/` nebo `http://server:4080/`

  (jméno serveru je pouze ilustrativní — viz kapitola 14).

  Alternativou je přihlášení k prohlížení webových statistik (viz kapitola 23) na adrese

  `https://server:4081/star` nebo `http://server:4080/star`

  Poznámka:
  Přihlášením do rozhraní *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 *Kerio Control* 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 18.1).

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 15.2).

  Přihlášení přesměrováním probíhá následovně: uživatel zadá do prohlížeče adresu stránky, kterou chce navštívit. *Kerio Control* 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.

- 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 27.4.

Upřesňující parametry pro ověřování uživatelů

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

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 *Kerio Control* (viz kapitola 14.2) a po úspěšném přihlášení na požadovanou WWW stránku.
- *Přístup přes proxy server v Kerio Control* — 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 15.2).

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 *Kerio Control* (podrobnosti viz kapitola 11.5) a v *Kerio Control* zapneme volbu *Povolit ověřování na netransparentním proxy serveru*. Proxy server pak bude vyžadovat ověření uživatele při zahájení každé nové relace prohlížeče[6].

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)

Při použití prohlížeče *Internet Explorer* nebo *Firefox/SeaMonkey* 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 27.4.

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).

[6] *Relace* (angl. *session*, někdy též překládáno jako *sezení*) je období běhu jedné instance prohlížeče. Např. v případě prohlížečů *Internet Explorer*, *Firefox* nebo *Google Chrome* 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).

Kapitola 14

WWW rozhraní

Kerio Control obsahuje speciální WWW server, který poskytuje rozhraní pro správu firewallu prostřednictvím WWW prohlížeče (*Kerio Control Administration*), pro prohlížení statistik a pro nastavení některých parametrů uživatelského účtu. Přístup k WWW rozhraní je zabezpečen protokolem SSL, aby nemohlo dojít k odposlechu síťové komunikace a odcizení uživatelských hesel a dalších citlivých informací.

WWW rozhraní firewallu otevřeme zadáním následujícího URL (`server` má význam jména nebo IP adresy počítače s *Kerio Control* a `4081` je port WWW rozhraní):

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

K dispozici je také nezabezpečené WWW rozhraní na portu `4080`:

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

Ve výchozím nastavení je nezabezpečené WWW rozhraní dostupné pouze na samotném firewallu na lokální zpětnovazební adrese (`localhost`, typicky `127.0.0.1`). Při přístupu na port `4080` z jiného počítače dojde k automatickému přesměrování na zabezpečené WWW rozhraní (`https://server:4081/`). Toto chování lze změnit v sekci

Konfigurace → *Další volby*, záložka *WWW rozhraní* (viz kapitola 14.1).

Porty WWW rozhraní nelze změnit.

Tato kapitola se zabývá konfigurací WWW rozhraní v administračním programu *Kerio Control*. Uživatelské WWW rozhraní je podrobně popsáno v manuálu *Kerio Control — Příručka uživatele*.

14.1 Informace o WWW rozhraní a nastavení certifikátu

WWW rozhraní *Kerio Control* lze nastavit v sekci *Konfigurace* → *Další volby*, záložka *WWW rozhraní*.

V horní části záložky jsou uvedeny odkazy na zabezpečené verze uživatelského WWW rozhraní firewallu a rozhraní pro správu (*Kerio Control Administration*). V dolní části lze získat informace o SSL certifikátu zabezpečeného WWW rozhraní a případně tento certifikát změnit.

Vypnutím volby *Použít zabezpečené připojení* lze povolit přístup k nezabezpečenému WWW rozhraní (včetně rozhraní pro správu) z libovolného počítače. Z bezpečnostních důvodů však doporučujeme tuto volbu nevypínat a vždy používat zabezpečené WWW rozhraní.

SSL certifikát pro WWW rozhraní

Princip zabezpečeného WWW rozhraní *Kerio Control* 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 *Kerio Control* je automaticky vytvořen testovací certifikát pro zabezpečené WWW rozhraní (certifikát je uložen v podadresáři `sslcert` instalačního adresáře *Kerio Control* 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.

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 (*).

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 *Kerio Control* 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.

14.2 Přihlašování uživatelů k WWW rozhraní

Při přístupu k WWW rozhraní *Kerio Control* je vyžadováno ověření uživatele. Do WWW rozhraní se může přihlásit každý uživatel, který má v *Kerio Control* vytvořen uživatelský účet. V závislosti na nastavení statistik (viz kapitola 23.2) se po přihlášení uživateli zobrazí jeho statistiky nebo stránka se stavovými informacemi a osobními předvolbami.

Při použití účtů z více než jedné domény (viz kapitola 18.4) 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 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 13.1.

Kapitola 15

Filtrování protokolů HTTP a FTP

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

15.1 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 9.3.

2. Kerio Control umožňuje filtrovat i šifrovanou komunikaci (protokol HTTPS). Lze však povolovat nebo blokovat přístup na celé servery, nikoliv již na jednotlivé stránky na nich.

3. Zabezpečenou FTP komunikaci (protokolem FTPS) není možné filtrovat. Protokol FTP rovněž nelze filtrovat při použití zabezpečeného přihlášení (*SASO*).

4. Pravidla pro HTTP i FTP se aplikují také při použití proxy serveru v *Kerio Control* (pak je podmínka 1. irelevantní). Protokol FTP však nelze filtrovat, pokud je použit nadřazený proxy server (podrobnosti viz kapitola 11.5). V takovém případě jsou pravidla pro FTP neaktivní.

5. Při použití proxy serveru (viz kapitola 11.5) je možné filtrovat také HTTPS servery (příklad: `https://secure.kerio.cz/`). Jednotlivé objekty na těchto serverech však již filtrovat nelze.

15.2 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*.

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 Control Web Filter* do určité kategorie atd.).
- *Vlastnosti* — upřesňující volby v pravidle (např. antivirová kontrola, filtrování zakázaných slov atd.).
- *Skupina IP adres* — skupina IP adres, pro kterou pravidlo platí. Jedná se o IP adresy klientů (tj. pracovních stanic uživatelů, kteří přes *Kerio Control* 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 *Kerio Control* obsahuje několik předdefinovaných pravidel pro URL. Tato pravidla jsou ve výchozím nastavení „vypnuta“. Správce firewallu 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.

Dvojitým kliknutím na jednotlivé položky (sloupce) nastavíme požadované parametry pravidla.

Jméno
Název/popis pravidla (pro lepší orientaci).

Akce, Vlastnosti
Akce pro stránky vyhovující tomuto pravidlu a doplňující nastavení pro vybranou akci:

- *Povolit* — povolení přístupu, uživatel nic nezaznamená.
  Pro stránky s povoleným přístupem lze nastavit tyto doplňkové kontroly / omezení:

- *Filtrovat z HTML kódu Java applety* (filtrování všech elementů `<applet>`),
- *Filtrovat z HTML kódu objekty ActiveX* (filtrování všech elementů `<embed>`),
- *Filtrovat z HTML kódu tagy Script* (filtrování všech elementů `<script>`),
- *Filtrovat z HTML kódu automatické otevírání nových oken* (tzv. pop-up blocker),
- *Filtrovat položky Referer z jiných domén* (často se používají pro sledování, odkud návštěvník na stránku přišel),
- *Zamezit přístup na stránky obsahující zakázaná slova v HTML kódu* (viz kapitola 15.4),
- *Neprovádět antivirovou kontrolu* (může zrychlit přístup na důvěryhodné stránky, obecně však doporučujeme antivirovou kontrolu provádět).

- *Zakázat* — uživatel bude přesměrován na stránku firewallu s informací o zakázaném přístupu.
  Je vhodné doplnit vysvětlující informaci, proč je přístup na danou stránku zakázán. Uživatelům s příslušným právem (viz kapitola 18.2) je možné povolit jednorázové „odemknutí“ zákazu. Všechna odemknutí budou zaznamenána do záznamu *Security* (viz kapitola 24.11).
- *Zahodit* — zákaz přístupu, uživateli se bude stránka jevit jako nedostupná.
- *Přesměrovat* — uživatel bude automaticky přesměrován na zadané URL (povinný parametr).

URL

URL adresa, pro kterou pravidlo platí:

- *URL začínající* — všechna URL, která začínají tímto řetězcem. Lze použít zástupné znaky `*` (hvězdička) a `?` (otazník).
  Sekvence znaků `*.` na začátku URL má speciální význam — doplňuje název počítače, případně subdomény v dané doméně, nebo název samotné domény.
  Příklad: Blokující pravidlo pro URL `*.kerio.cz` zablokuje přístup na adresy `http://www.kerio.cz/`, `http://mail.kerio.cz/` i `http://kerio.cz/`, nikoliv však na `http://www.mojekerio.cz/` ani na `http://mojekerio.cz/`.
- *URL ze skupiny* — všechna URL z vybrané skupiny URL.
- *URL kategorizované modulem Kerio Control Web Filter* — všechny stránky, které byly modulem *Kerio Control Web Filter* zařazeny do vybraných kategorií.
- *Libovolné URL, ve kterém je server zadán IP adresou* (zkušenější uživatelé mohou tímto způsobem obcházet pravidla pro URL). Lze použít pouze pro nezabezpečenou komunikaci (protokol HTTP).
- *Protokol* — standardně se filtruje nezabezpečená komunikace (protokol HTTP). Kerio Control umožňuje filtrovat i zabezpečená spojení (HTTPS), avšak pouze na základě jména serveru. Zbývající část podmínky pro URL je ignorována. Je tedy možné povolit nebo blokovat přístup na konkrétní server, nikoliv však na jednotlivé stránky na daném serveru.
  Blokování protokolu zabezpečené komunikace (HTTPS) nelze z technických

důvodů aplikovat na klienty používající prohlížeč Internet Explorer na systému Windows XP.

MIME typ
MIME typ objektů (stahovaných souborů), pro které má pravidlo platit. Lze použít zástupný symbol * (hvězdička). Samotná hvězdička znamená libovolný MIME typ.

Zdroj
Skupina IP adres klientů (uživatelských počítačů), pro která má pravidlo platit.
Nastavením hodnoty *Libovolný* bude omezení na IP adresy zrušeno.

Časová platnost
Časový interval, ve kterém má pravidlo platit.

Záznam
Zapnutí / vypnutí zápisu všech HTTP požadavků vyhovujících tomuto pravidlu do záznamu *Filter* (viz kapitola 24.9).

Upřesňující parametry pro inspekci protokolu HTTP

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 9) 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.

15.3 Hodnocení obsahu WWW stránek (Kerio Control Web Filter)

Modul *Kerio Control Web Filter*, integrovaný v *Kerio Control*, 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 Control 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 Control Web Filter* v *Kerio Control* 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 Control Web Filter* je vázáno na speciální licenci. Pokud licence *Kerio Control* neobsahuje tento modul, chová se modul jako zkušební verze (po 30 dnech od instalace *Kerio Control* se automaticky vypne a volby v záložce *Kerio Control Web Filter* budou neaktivní). Podrobné informace o licencích naleznete v kapitole 5.

Nastavení parametrů modulu Kerio Control Web Filter

K aktivaci/deaktivaci a nastavení upřesňujících parametrů modulu *Kerio Control Web Filter* slouží záložka *Kerio Control Web Filter* v sekci *Konfigurace* → *Filtrování obsahu* → *Pravidla pro HTTP*.

Povolit Kerio Control Web Filter

Tato volba zapíná/vypíná modul pro klasifikaci WWW stránek *Kerio Control Web Filter*.
Je-li modul *Kerio Control Web Filter* vypnut, pak:

- nejsou dostupné ostatní volby v záložce *Kerio Control Web Filter*,
- jsou deaktivována všechna pravidla pro URL, která používají klasifikaci modulem *Kerio Control Web Filter* (podrobnosti viz kapitola 15.2).

Kategorizovat každou stránku bez ohledu...

Po zapnutí této volby budou modulem *Kerio Control 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 23). Nechceme-li tyto statistiky sledovat, doporučuje se tuto volbu vypnout (kategorizace všech stránek by zbytečně snižovala výkon *Kerio Control*).

Povolit ověřeným uživatelům nahlásit nesprávnou kategorizaci...

Pokud se uživatel domnívá, že je stránka zařazena do nesprávné kategorie (a tudíž je mu na ni neprávem blokován přístup), může navrhout změnu kategorizace této stránky. Návrh bude vyhodnocen správci databáze během několika dnů.
Z bezpečnostních důvodů mohou návrhy na změnu kategorizace zasílat pouze ověření uživatelé. Všechny návrhy na změnu kategorizace budou zaznamenány do záznamu *Security* (viz kapitola 24.11).

Test kategorizace URL

Přímo v rozhraní Kerio Control Administration je možné otestovat kategorizaci zadané stránky (URL). Na stránce s výsledkem je pak možné navrhnout změnu kategorizace.

V poli *Výjimky pro Kerio Control 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 Control 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 nahrazuje 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 Control Web Filter

Pro klasifikaci WWW stránek modulem *Kerio Control Web Filter* musí být tento modul zapnut a nastaveny jeho parametry.

Modul *Kerio Control Web Filter* se aktivuje vždy, když *Kerio Control* 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*, povolíme předdefinované pravidlo *Deny sites rated in Kerio Control Web Filter Categories* (viz kapitola 15.2).

Dvakrát klikneme na pole ve sloupci *URL* a tlačítkem *Vybrat hodnocení* otevřeme dialog pro výběr kategorií modulu *Kerio Control Web Filter* a zvolíme kategorii *Zaměstnání / Nabídky zaměstnání* (stránky s nabídkami pracovních míst).

Poznámka:

1. Pravidel pro URL využívajících *Kerio Control Web Filter* může být definováno více. V každém pravidle může být nastaveno více kategorií.
2. V pravidlech používajících klasifikaci modulem *Kerio Control 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 je možné zkontrolovat, zda byl požadavek uživatele oprávněný či nikoliv.

15.4 Filtrování WWW stránek dle výskytu slov

Kerio Control 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 *Kerio Control* definovat tzv. zakázaná slova. Pomocí pravidel pro URL (viz kapitola 15.2) 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. Dvakrát klikneme na pole ve sloupci *Vlastnosti* a zaškrtneme volbu *Zamezit přístup na stránky obsahující zakázaná slova v HTML kódu.*

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.

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 *Kerio Control* 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 firewallu 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.

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).

15.5 Filtrování protokolu FTP

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

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

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

- *Forbid resume due to antivirus scanning* — zákaz pokračování ve stahování souboru po přerušení (tzv. *resume* — FTP příkaz `REST`).
  Toto pravidlo může zvýšit účinnost antivirové kontroly (soubor bude vždy kontrolován jako celek). Při přenosu velkých souborů však může být kontraproduktivní — pravděpodobnost, že kód viru se nachází právě v místě, kde došlo k přerušení, je velmi malá, a opakování přenosu celého souboru zbytečně zatěžuje internetové připojení.
  Podrobnosti o antivirové kontrole protokolu FTP naleznete v kapitole 16.3.
- *Forbid upload* — zákaz ukládání souborů na FTP servery. Tímto lze zablokovat jednu z cest úniku citlivých informací z lokální sítě.
- Dvě pravidla pro zákaz stahování audio a video souborů — tyto soubory bývají objemné a jejich stahování neúměrně zatěžuje internetové připojení. Navíc se zpravidla jedná o neproduktivní činnost.

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.

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.

Jednotlivé parametry pravidla nastavíme dvojitým kliknutím na příslušnou položku (sloupec):

Jméno
Název/popis pravidla (pro lepší orientaci).
Zaškrtávací pole vedle jména pravidla slouží k jeho „vypnutí“ — pravidlo můžete dočasně vyřadit bez nutnosti jej odstraňovat a poté znovu přidávat.

Akce
Typ pravidla — povolení nebo zákaz přístupu.

Vlastnosti
Doplňková nastavení pro zvolenou akci:

- Povolení přístupu — volitelně lze vypnout antivirovou kontrolu přenášených souborů (doporučujeme používat pouze v odůvodněných případech a pro důvěryhodné FTP servery!).
- Zákaz přístupu — žádná doplňková nastavení nejsou k dispozici.

Server
FTP servery, pro které pravidlo platí:

- Libovolný FTP server,
- Specifický FTP server — může být zadán DNS jménem nebo IP adresou,
- Všechny FTP servery z vybrané skupiny IP adres (viz kapitola 17.1).

Podmínka
Podmínka pravidla:

- *Cokoliv* — pravidlo platí pro veškerou FTP komunikaci vyhovující ostatním parametrům (*Server*, *Uživatelé*, *Zdroj*, *Časová platnost*).
- *Ukládání* — pravidlo platí pro ukládání (upload) specifikovaných souborů na FTP server. V názvu souboru lze použít zástupné znaky * (hvězdička) a ? (otazník). Samotná hvězdička znamená libovolný soubor.
- *Stahování* — pravidlo platí pro stahování (download) specifikovaných souborů z FTP serveru.
- *Stahování / Ukládání* — pravidlo platí pro stahování (download) i ukládání specifikovaných souborů z/na FTP server.
- *FTP příkaz* — pravidlo je aplikováno na specifické příkazy protokolu FTP. Požadované příkazy lze vybrat ze seznamu, případně tlačítkem *Přidat* definovat vlastní příkaz.

Uživatelé
Výběr uživatelů a/nebo skupin, pro které má pravidlo platit.

Zdroj
Skupina IP adres klientů (uživatelských počítačů), pro která má pravidlo platit (viz kapitola 17.1).
Nastavením hodnoty *Libovolný* bude omezení na IP adresy zrušeno.

Časová platnost
Časový interval, ve kterém má pravidlo platit (viz kapitola 17.2).

Záznam
Zapnutí / vypnutí zápisu všech FTP operací vyhovujících tomuto pravidlu do záznamu *Filter* (viz kapitola 24.9).

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 17.2).

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 17.1).

Obsah
Upřesňující volby pro obsah FTP komunikace.
Volba *Typ* nastavuje způsob filtrování:

- *Download*, *Upload*, *Download / Upload* přenos souborů v některém směru, případně v obou směrech.
  Při výběru některé z těchto voleb se zobrazí položka *Jméno souboru* — v této položce můžete uvést jména souborů, pro které má pravidlo platit. Ve jméně souboru lze použít hvězdičkovou konvenci (např. `*.exe` — spustitelné soubory).
- *FTP příkaz* — výběr příkazů protokolu FTP, pro které má pravidlo platit
- *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 16

Antivirová kontrola

Kerio Control umožňuje provádět antivirovou kontrolu objektů (souborů) přenášených protokoly HTTP, FTP, SMTP a POP3. V případě protokolů HTTP a FTP může správce firewallu specifikovat, které objekty (resp. typy objektů) mají být kontrolovány.

Kerio Control je dodáván s integrovaným antivirem *Sophos*. Použití antiviru vyžaduje speciální licenci.

16.1 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 17.3) 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 16.4.

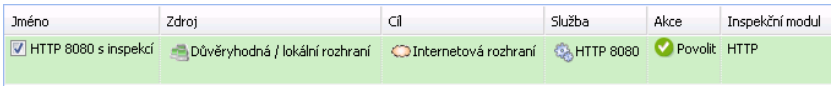
- Objekty přenášené jinými protokoly než HTTP, FTP, SMTP a POP3 nelze kontrolovat antivirem.

- 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 9.3).

  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 16.1 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“).

16.2 Nastavení antivirové kontroly

K nastavení antivirové kontroly v Kerio Control slouží sekce *Konfigurace* → *Filtrování obsahu* → *Antivirus*.

Konfigurace integrovaného antivirového modulu

Chceme-li použít integrovaný antivirus *Sophos*, zapneme v horní části záložky *Antivirový modul* volbu *Použít Integrovaný antivirový modul*. Tato volba je dostupná pouze v případě, že licenční klíč *Kerio Control* obsahuje licenci pro antivirový modul *Sophos*, nebo jedná-li se o zkušební verzi *Kerio Control*. Podrobné informace o licencích naleznete v kapitole 5.

V dolní části záložky *Antivirový modul* je nyní aktivní sekce *Integrovaný antivirový modul*, ve které lze nastavit aktualizaci modulu *Sophos*.

Zkusit aktualizovat každých ... hodin

Tato volba zapíná/vypíná automatickou kontrolu nových verzí virové databáze a antivirového programu v nastaveném intervalu.
V těchto intervalech *Kerio Control* ověří, 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 24.8).
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 *Sophos*, který *Kerio Control* používá.

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

Parametry kontroly protokolů a souborů

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.

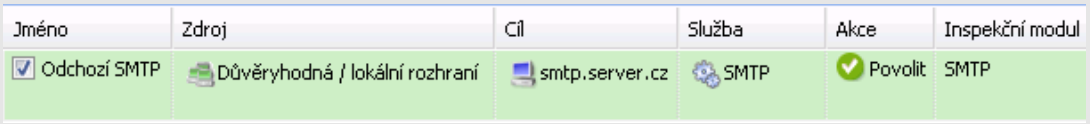
V poli *Nastavení* lze určit maximální velikost souborů, které budou antivirem na firewallu kontrolovány. Kontrola velkých souborů je náročná na čas, procesor i diskový prostor serveru, což může mít zásadní negativní vliv na činnost firewallu. V některých případech může také dojít k přerušení spojení, kterým je soubor přenášen, z důvodu vypršení časového limitu.

Optimální hodnota je závislá na konkrétních podmínkách (výkon serveru, intenzita síťového provozu, charakter přenášených dat atd.). *Důrazně doporučujeme neměnit výchozí nastavení omezení velikosti souboru, v žádném případě nenastavovat vyšší hodnotu než výchozí (4 MB).*

Parametry kontroly protokolů HTTP a FTP lze nastavit v záložce *Kontrola HTTP a FTP* (viz kapitola 16.3), parametry kontroly SMTP a POP3 v záložce *Kontrola e-mailu* (viz kapitola 16.4).

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 16.2.



Obrázek 16.2 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. *Kerio Control* pak nemůže provádět antivirovou kontrolu jednotlivých příloh.
   V těchto případech doporučujeme použít antivirový program, který spolupracuje přímo s *Microsoft Exchange*, a v *Kerio Control* 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 9.8).

16.3 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) *Kerio Control* pozdrží ve své vyrovnávací paměti a provede antivirovou kontrolu souboru v dočasném adresáři. Je-li v souboru nalezen virus, pak *Kerio Control* poslední blok dat zahodí. Klient tak dostane soubor poškozený (neúplný) — nebude jej moci spustit a virus aktivovat. Není-li nalezen žádný virus, pak *Kerio Control* 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 15.2 a 15.5.
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*.

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 na firewallu do speciálního adresáře. Správce firewallu 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 instalačním adresáři *Kerio Control*:

  Na systému Windows: `C:\Program Files\Kerio\WinRoute Firewall\quarantine`

  V ostatních edicích: `/opt/kerio/winroute/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 *Kerio Control*!

- *Upozornit klienta* — *Kerio Control* pošle uživateli, který tento soubor stahoval, e-mailovou zprávu s výstrahou, že v tomto souboru byl detekován virus a stahování bylo přerušeno.

Výstrahu *Kerio Control* vyšle pouze za těchto podmínek: uživatel je přihlášen na firewall, v příslušném uživatelském účtu je nastavena platná e-mailová adresa (viz kapitola 18.1) a je korektně nastaven SMTP server pro odesílání pošty (viz kapitola 20.3).

Poznámka:
Nezávisle na volbě *Upozornit klienta* lze při detekci virů zasílat výstrahy na definované adresy (např. správcům sítě). Podrobnosti naleznete v kapitole 21.5.

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* — *Kerio Control* bude tyto soubory považovat za infikované a nepovolí jejich přenos.

  Tip
  Tuto volbu je vhodné kombinovat s volbou *Přesunout soubor do karantény* — správce firewall pak může např. ve spolupráci s příslušným uživatelem soubor dekomprimovat a provést antivirovou kontrolu ručně.

- *Povolit přenos souboru* — *Kerio Control* 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.

Kerio Control 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 firewallu 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.

Popis
Textový popis pravidla (pro snazší orientaci správce firewallu).

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 antivirem.
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 antivirem 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*).

16.4 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 *Kerio Control* 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 21.5.

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 16.2.

Záložka *Antivirová kontrola e-mailu* umožňuje nastavit akce při nalezení viru a upřesňující parametry.

V poli *Obsahuje-li zpráva přílohy odmítnuté antivirovou kontrolou* lze nastavit akce pro zprávu, ve které byla nalezena alespoň jedna infikovaná příloha:

- *Uložit zprávu do karantény* — zpráva bude uložena do speciálního adresáře na počítači s *Kerio Control*. Správce firewallu se pak může pokusit infikované přílohy léčit antivirovým programem a v případě úspěchu je předat původnímu adresátovi.

  Pro karanténu se používá podadresář `quarantine` v instalačním adresáři *Kerio Control*:

  Na systému Windows: `C:\Program Files\Kerio\WinRoute Firewall\quarantine`

  V ostatních edicích: `/opt/kerio/winroute/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 firewallu 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 antivirem (např. archiv chráněný heslem, poškozený soubor apod.):

- *Zakázat doručení této přílohy — Kerio Control* se zachová stejně jako v případě detekce viru (včetně výše popsaných akcí).

- *Povolit doručení této přílohy — Kerio Control* 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.

16.5 Kontrola souborů přenášených Clientless SSL-VPN (Windows)

Je-li *Kerio Control* 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 26). Záložka *Kontrola SSL-VPN* umožňuje nastavit upřesňující parametry pro kontrolu souborů přenášených tímto rozhraním. Při správě *Kerio Control* v edicích *Appliance* a *Box* 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 antivirus určitý soubor z nějakého důvodu zkontrolovat (typicky šifrovaný archiv nebo poškozený soubor). Ve výchozí konfiguraci je z bezpečnostních důvodů přenos takových souborů zakázán.

Kapitola 17

Definice

17.1 Skupiny IP adres

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

Vytvoření či úprava skupiny IP adres

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

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

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

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

Typ
: Druh přidávané položky:

- *Počítač* (IP adresa nebo DNS jméno konkrétního počítače),
- *Síť / maska* (subsíť s příslušnou maskou),
- *Rozsah IP adres* (interval zadaný počáteční a koncovou adresou včetně),
- *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 9.3).

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.

17.2 Časové intervaly

Časové intervaly jsou v *Kerio Control* úzce propojeny s komunikačními pravidly (viz kapitola 9). Správce firewallu má tak možnost nastavit časové období, kdy bude dané pravidlo platit. Ve skutečnosti se nejedná o jeden časový úsek, ale o skupinu tvořenou libovolným počtem různých intervalů a/nebo jednorázově naplánovaných akcí.

Druhým využitím časových intervalů je nastavení parametrů vytáčených linek — viz kapitola 7.

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

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

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).

17.3 Služby

Služby v *Kerio Control* 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 *Kerio Control* je zde již předdefinována řada standardních služeb (např. HTTP, FTP, DNS atd.).

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

Jméno

Identifikace služby v rámci *Kerio Control*. 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 *Kerio Control* 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).

Inspekční modul

Inspekční modul *Kerio Control* (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 9.3.

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)
- *Seznam* — seznam portů oddělených čárkami (např.: `80,8000,8080`)

Inspekční moduly

Kerio Control 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 *Kerio Control* 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 *Kerio Control* bude automaticky aplikován inspekční modul protokolu *HTTP*.

Poznámka:

1. Inspekční moduly obecně nelze použít pro zabezpečenou komunikaci (SSL/TLS). V tomto případě *Kerio Control* „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 9.8.

17.4 Skupiny URL

Skupiny URL slouží ke snadné a přehledné definici pravidel pro HTTP (viz kapitola 15.2). 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 *Kerio Control* 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 15.2). Správce firewallu 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.

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 18

Uživatelské účty a skupiny

Uživatelské účty v *Kerio Control* slouží pro lepší řízení přístupu uživatelů z lokální sítě ke službám v Internetu. Uživatelský účet může být použit také pro přístup ke správě *Kerio Control*.

Kerio Control 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 v *Kerio Control*, 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 (*Active Directory*, *Open Directory* nebo *Windows NT*) však představují lokální účty v *Kerio Control* značné zvýšení administrativních nároků — účty a hesla je nutné udržovat na dvou místech (doménový server a *Kerio Control*).

Interní databáze uživatelů s ověřováním v doméně

Uživatelské účty jsou uloženy v *Kerio Control*, ale uživatelé se ověřují v doméně (tzn. v uživatelském účtu v *Kerio Control* není uloženo heslo). Uživatelské jméno v *Kerio Control* a v doméně musí být totožné.

Z hlediska administrativy je tento způsob uložení účtů a ověřování uživatelů méně náročný než lokální účty — pokud si např. uživatel chce změnit heslo, stačí jej změnit v doméně a tato změna se automaticky promítne také do účtu v *Kerio Control*. Uživatelské účty v *Kerio Control* navíc není nutné vytvářet ručně, lze je importovat z příslušné domény (*Windows NT* nebo *Active Directory*).

Transparentní spolupráce s adresářovou službou (mapování domén)

Kerio Control může používat přímo účty a skupiny uložené v *Active Directory* nebo *Open Directory* — neprovádí se žádný import do lokální databáze. Specifické parametry pro *Kerio Control* 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 adresářové službě) a jako jediný umožňuje použití účtů z více různých domén.

Poznámka:
V případě ověřování uživatelů v doméně (tj. druhý a třetí způsob) je doporučeno vytvořit v *Kerio Control* 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 *Kerio Control* i při výpadku sítě nebo doménového serveru.

18.1 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*.

Doména
Volba *Doména* umožňuje vybrat doménu, pro kterou budeme definovat uživatelské účty a další parametry. V této položce lze zvolit některou z mapovaných domén (viz kapitola 18.4) nebo lokální (interní) databázi uživatelů.

Vyhledávání
V horní části okna je možné zadat filtr pro zobrazení uživatelských účtů. Po stisknutí klávesy *Enter* se zobrazí všechny účty obsahující zadaný řetězec znaků v položce *Jméno*, *Celé jméno* nebo *Popis*. Filtr lze zrušit vymazáním pole a opětovným stisknutím klávesy *Enter*.
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 v *Kerio Control* 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 18.2).

Lokální uživatelské účty

Volbou *Lokální databáze uživatelů* v položce *Doména* se zobrazí lokální uživatelské účty v *Kerio Control* (všechny informace o těchto účtech jsou uloženy v konfigurační databázi *Kerio Control*). 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 18.2). 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 18.3.

Import účtů je vhodné použít v případě domény *Windows NT*. V případě domény *Active Directory* nebo *Open Directory* je výhodnější využít transparentní spolupráci (tzv. mapování domén — viz kapitola 18.4).

Mapované účty z domény

Výběrem některé z mapovaných domén v položce *Doména* se zobrazí seznam uživatelských účtů v této doméně.

Změna účtu

U mapovaných účtů lze nastavit parametry specifické pro *Kerio Control* (podrobnosti viz kapitola 18.2). Tato nastavení budou uložena do konfigurační databáze *Kerio Control*. Údaje uložené v adresářové službě (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 doménách nelze vytvářet ani rušit uživatelské účty. Tyto akce musí být prováděny přímo na příslušném doménovém serveru. Rovněž není možný import uživatelských účtů — taková akce nemá v případě mapované domény smysl.

18.2 Lokální uživatelské účty

Lokální účty jsou účty vytvořené v *Kerio Control* nebo importované z domény. Tyto účty jsou uloženy v konfigurační databázi *Kerio Control* (viz kapitola 27.3). 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 *Kerio Control*, v *Active Directory* nebo v doméně *Windows NT*.

Základní administrátorský účet `Admin` se vytváří přímo během instalace *Kerio Control*. Tento účet má plná práva 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 *Kerio Control*, nebude již možné se ke správě znovu přihlásit. V takovém případě bude při dalším startu *Kerio Control Engine* automaticky vytvořen lokální uživatelský účet `Admin` s prázdný heslem.
3. V případě zapomenutí administrátorského hesla kontaktujte technickou podporu firmy *Kerio Technologies*.

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 dialog pro vytvoření nového uživatelského účtu.

Obecné — základní údaje

Jméno

Přihlašovací jméno uživatele.

> ***Upozornění:***
> V uživatelském jméně se nerozlišují malá a velká písmena. Nedoporučuje se používat v uživatelském jméně české znaky (tj. písmena s diakritikou) — mohlo by dojít k problémům s přihlašováním 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 21.5) a dalších zpráv (např. varování o překročení limitu objemu přenesených dat). Pro efektivní využití všech funkcí *Kerio Control* je třeba každému uživateli nastavit platnou e-mailovou adresu.

Poznámka:
Pro zasílání e-mailových zpráv uživatelům musí být v *Kerio Control* nastaven server odchozí pošty. Podrobnosti naleznete v kapitole 20.3.

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 18.1) 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 *Kerio Control*). 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 *Kerio Control*. 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 Control — 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 27.4). Tyto účty rovněž nelze použít pro přístup do rozhraní *Clientless SSL-VPN* (viz kapitola 26).

Adresářová služba

Uživatel bude ověřován v mapované doméně adresářové služby *Active Directory* nebo *Open Directory*, případně v doméně *Windows NT*, jejímž je firewall členem.
Poznámka:
Není-li správně nastavena doména, pak budou uživatelské účty s ověřováním v doméně neaktivní. Podrobnosti viz kapitola 18.3.

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 18.5). 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*.

Přístupová práva

Každý uživatel musí mít nastavenu jednu ze tří úrovní přístupových práv.

Nemá přístup ke správě

Uživatel nemá práva pro přihlášení ke správě *Kerio Control*. 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 *Kerio Control*, 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...

Toto právo ovlivňuje způsob použití voleb pro filtrování objektů na WWW stránkách (podrobnosti viz *Krok 5*):

- Pokud pro danou stránku *existuje* pravidlo pro URL (viz kapitola 15.2) a uživatel *nemá* toto právo, pak bude použito nastavení z příslušného pravidla pro URL a nastavení v uživatelském účtu bude ignorováno.
- Pokud pro danou stránku *existuje* pravidlo pro URL a uživatel *má* toto právo, pak bude použito nastavení z uživatelského účtu a nastavení v příslušném pravidle pro URL bude ignorováno.
- Pokud pro danou stránku *neexistuje* pravidlo pro URL, pak bude použito nastavení z uživatelského účtu a na tomto právu nezáleží.

Uživatel může „odemykat“ pravidla pro URL
Toto právo uživateli povoluje 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 15.2).

Uživatel může vytáčet telefonické připojení
Pokud je připojení k Internetu realizováno vytáčenými linkami, uživatel bude moci tyto linky vytáčet a zavěšovat prostřednictvím WWW rozhraní firewallu (viz kapitola 14).

Uživatel se může připojovat k VPN serveru
Uživatel má právo připojit se k VPN serveru v *Kerio Control* (aplikací *Kerio VPN Client*). Podrobné informace naleznete v kapitole 25.

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 v *Kerio Control* pro systém *Windows*. Podrobnosti viz kapitola 26.

Uživatel může používat P2P sítě
Na tohoto uživatele nebude aplikováno blokování komunikace při detekci *P2P* (*Peer-to-Peer*) sítí. Podrobnosti viz kapitola 10.4.

Uživatel má právo prohlížet statistiky
Tento uživatel bude mít přístup ke statistikám firewallu zobrazovaným ve WWW rozhraní (viz kapitola 14).

> ***Tip***
> Přístupová práva mohou být nastavena šablonou uživatelského účtu.

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 12.

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). V *Kerio Control* musí být nastaven server odchozí pošty (viz kapitola 20.3).
Má-li být při překročení kvóty některým uživatelem varován také správce *Kerio Control*, můžeme nastavit příslušnou výstrahu v sekci *Konfigurace* → *Statistiky a výstrahy*. Podrobnosti naleznete v kapitole 21.5.
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 22.1).
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.

Předvolby — pravidla pro obsah WWW stránek a preferovaný jazyk

V tomto kroku je možné provést specifické nastavení filtrování objektů na WWW stránkách pro konkrétního uživatele. Ve výchozím nastavení jsou všechny prvky povoleny.

Použití těchto pravidel závisí na uživatelském právu *Přejít pravidla pro obsah WWW stránek* a na tom, zda pro konkrétní stránku existuje pravidlo pro URL či nikoliv. Podrobnosti viz *Krok 3* (uživatelská práva).

Kerio Control 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 *Kerio Control*. Volba *podle prohlížeče* znamená, že *Kerio Control* 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 *Kerio Control* (viz manuál *Kerio Control — Příručka uživatele*).

Tip
Pravidla pro obsah WWW stránek mohou být nastavena šablonou uživatelského účtu.

IP adresy uživatele

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 *Kerio Control* 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. *Kerio Control* 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 *Kerio Control* 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 17.1).

> ***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 25.

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.

18.3 Lokální databáze uživatelů: ověřování v adresářové službě a import účtů

Uživatelé v lokální databázi mohou být ověřováni adresářové službě (viz kapitola 18.2, první krok průvodce). Pro použití těchto způsobů ověřování musí být počítač s *Kerio Control* členem příslušné domény.

Je-li *Kerio Control* nainstalován na systému *Windows*, lze počítač přidat do domény nebo změnit členství v doméně pouze v operačním systému (ve vlastnostech počítače).

V edicích *Appliance* a *Box* je možné nastavit členství v doméně přímo ve správě firewallu, a to v sekci *Domény a přihlašování uživatelů*, záložka *Adresářové služby*. *Kerio Control* v této edici 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 v *Kerio Control* na systému *Windows*. Z domény *Open Directory* nelze uživatelské účty importovat.

Import uživatelského účtu znamená vytvoření lokálního účtu se stejným uživatelským jménem a ověřováním v příslušné doméně. Specifické parametry pro *Kerio Control* (např. přístupová práva, pravidla pro obsah WWW stránek, kvóty objemu přenesených dat apod.) budou nastaveny podle šablony pro lokální databázi uživatelů (viz kapitola 18.1), případně je lze u vybraných účtů nastavit individuálně. U všech importovaných účtů bude nastaven typ ověřování *Adresářová služba*.

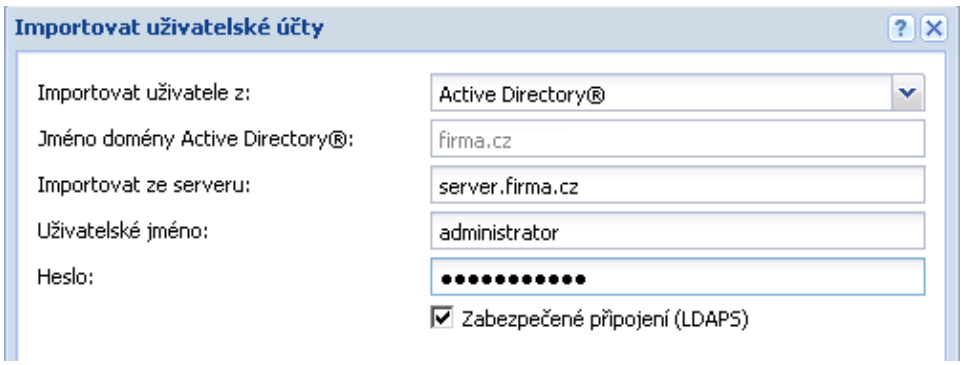
Poznámka:
Tento způsob importu uživatelských účtů je vhodný zejména při použití *Windows NT* domény (doménový server s operačním systémem *Windows NT Server*). V případě domény *Active Directory* je výhodnější a jednodušší je použít mapování domény — viz kapitola 18.4.

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).

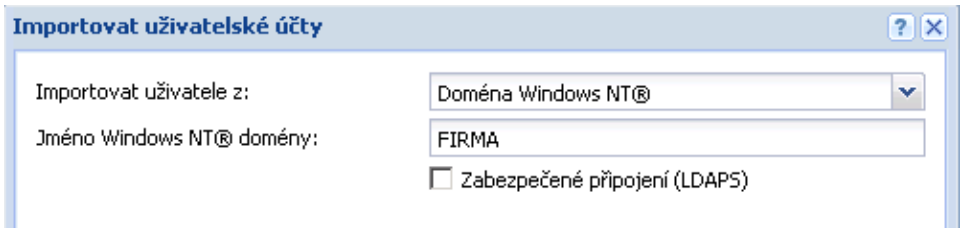
V dialogu pro import účtů je nejprve třeba zvolit typ domény, z níž mají být účty importovány, a podle typu domény pak zadat příslušné parametry:

- *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 18.1 Import účtů z Active Directory

- *NT doména* — pro import účtů musí být zadáno jméno domény. Počítač s *Kerio Control* musí být členem této domény.



Obrázek 18.2 Import účtů z domény Windows NT

Poznámka:
Import uživatelských účtů z domény *Windows NT* lze provést pouze v *Kerio Control* 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.

18.4 Uživatelské účty v adresářové službě — mapování domén

V *Kerio Control* lze přímo používat uživatelské účty z jedné nebo více domén *Active Directory* nebo *Open Directory*. Tato funkce se nazývá mapování domén. Hlavní výhodou je, že veškerá správa uživatelských účtů a skupin probíhá pouze v adresářové službě (s použitím standardních systémových nástrojů). Pro každou doménu definovat šablonu, podle které budou nastaveny parametry účtů specifické pro *Kerio Control* (přístupová práva, kvóty objemu dat a pravidla pro obsah WWW stránek — viz kapitola 18.1). V případě potřeby lze u konkrétních účtů tyto parametry nastavit individuálně.

Poznámka:
Doménu *Windows NT* nelze popsaným způsobem mapovat. V případě domény *Windows NT* doporučujeme importovat uživatelské účty do lokální databáze uživatelů (viz kapitola 18.3)

Nastavení mapování domén

Mapování domén lze nastavit v sekci *Uživatelé a skupiny* → *Domény a přihlašování uživatelů*, záložka *Adresářové služby*.

Podmínky použití mapovaných domén Active Directory

Pro správnou funkci ověřování uživatelů v mapovaných doménách *Active Directory* musí být splněny tyto podmínky:

- V případě jedné mapované domény:

1. Počítač s *Kerio Control* musí být členem příslušné *Active Directory* domény.

2. Počítače v lokální síti (pracovní stanice uživatelů) by měly jako primární DNS server používat modul *DNS* v *Kerio Control*, 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 *Kerio Control* musí být členem jedné z mapovaných domén. Tato doména bude označována jako primární.

  2. Primární doména musí důvěřovat všem ostatním doménám, které jsou v *Kerio Control* 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 modul *DNS* v *Kerio Control*).

Připojení firewallu do domény Active Directory (edice Appliance a Box)

Horní část záložky *Adresářové služby* zobrazuje informaci o členství počítače s firewallem v doméně a umožňuje přidat firewall do domény *Active Directory*, změnit jeho členství v doméně nebo jej odpojit od domény.

Nejprve je potřeba zvolit adresářovou službu *Active Directory* a zadat celé jméno domény (např. `firma.cz`).

Tlačítkem *Přidat do domény* se pak spustí jednoduchý průvodce, ve kterém je potřeba zadat ještě jméno počítače (firewallu) a heslo uživatele s právem přidávat počítače do domény.

Pokud se *Kerio Control* 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).

Upřesňující nastavení

Způsob spolupráce *Kerio Control* s adresářovými službami lze ovlivnit několika upřesňujícími parametry.

Zabezpečené připojení k doménovému serveru

Pro zvýšení bezpečnosti (znemožnění odposlechu komunikace a získání hesel uživatelů) může být komunikace s adresářovým serverem šifrována. Povolení šifrovaného spojení vyžaduje odpovídající nastavení na příslušném doménovém serveru (resp. na všech serverech dané domény, pokud je použita automatická detekce).

Active Directory: 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 *Kerio Control*. 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 *Kerio Control* 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*. V edicích *Appliance* a *Box* 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 aplikace *Kerio Control* (resp. *Kerio WinRoute Firewall*). 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 *Kerio WinRoute Firewall* (verze *6.7.0* nebo nižší).

Mapování dalších domén

Chceme-li mapovat uživatelské účty z několika různých 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.

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 adresářové služby s lokální databází a konverze účtů

Při mapování domény adresářové služby 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 adresářové služby.

Při konverzi účtu budou automaticky provedeny tyto operace:

- nahrazení všech výskytů lokálního účtu v konfiguraci *Kerio Control* (v komunikačních pravidlech, pravidlech pro URL, pravidlech pro FTP atd.) odpovídajícím účtem z adresářové služby,
- kombinace práv lokálního a doménového účtu,
- 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 adresářové služby 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 adresářové službě (i v případě, že je jméno lokální skupiny shodné se jménem skupiny v příslušné doméně).

18.5 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*.

Doména

Volba *Doména* umožňuje vybrat doménu, pro kterou budeme definovat skupiny uživatelů nebo nastavovat jejich parametry. V této položce lze zvolit některou z mapovaných domén (viz kapitola 18.4) nebo lokální databázi uživatelů.

V *Kerio Control* lze vytvářet skupiny pouze v lokální databázi uživatelů. Nelze je vytvářet v mapovaných doménách. Rovněž není možné importovat skupiny z domény do lokální databáze.

V případě skupin v mapovaných doménách lze pouze nastavit přístupová práva (viz dále — 3. krok průvodce vytvořením skupiny uživatelů).

Vyhledávání

V horní části okna je možné zadat filtr pro zobrazení skupin uživatelů účtů. Po stisknutí klávesy *Enter* se zobrazí všechny skupiny obsahující zadaný řetězec znaků v položce *Jméno* nebo *Popis*. Filtr lze zrušit vymazáním pole a opětovným stisknutím klávesy *Enter*. 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 v dialogu, který se zobrazí po stisknutí tlačítka *Přidat*.

Obecné — název a popis skupiny

Jméno

Název skupiny (jednoznačně identifikuje skupinu)

Popis

Textový popis skupiny (má pouze informativní charakter, může obsahovat libovolné informace nebo zůstat prázdný)

Členové skupiny

Tlačítky *Přidat* a *Odebrat* lze přidat či odebrat uživatele do/z této skupiny. Nejsou-li uživatelské účty dosud vytvořeny, může skupina zůstat prázdná a uživatelé do ní budou zařazeni při definici účtů (viz kapitola 18.1).

> ***Tip***
> Při přidávání uživatelů lze označit více uživatelských účtů najednou přidržením klávesy *Ctrl* nebo *Shift*.

Práva — 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 *Kerio Control*.

Přístup jen pro čtení
Uživatelé v této skupině se mohou přihlásit ke správě *Kerio Control*, 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 nastavuje způsob aplikace pravidel pro prvky WWW stránek, pokud pro danou stránku existuje pravidlo pro URL. Podrobnosti viz popis tohoto práva v kapitole 18.2.

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 15.2). 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 14).

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 25).

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 v *Kerio Control* pro systém *Windows*. Podrobnosti viz kapitola 26.

Uživatelé mohou používat P2P sítě
Na členy této skupiny nebude aplikován modul *P2P Eliminator* (detekce a blokování *Peer-to-Peer* sítí — viz kapitola 10.4).

Uživatelé mohou prohlížet statistiky
Členové této skupiny budou mít přístup ke statistikám firewallu zobrazovaným ve WWW rozhraní (viz kapitola 14).

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 19

Administrativní nastavení

19.1 Systémová konfigurace (edice Appliance a Box)

V edicích *Appliance* a *Box* umožňuje konzole pro správu *Kerio Control* 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*.

Datum, čas a časová zóna

Pro celou řadu funkcí *Kerio Control* (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`.

19.2 Automatická aktualizace produktu

Kerio Control může v pravidelných intervalech kontrolovat, zda se na serveru firmy Kerio Technologies nachází novější verze produktu, než je aktuálně nainstalována. Kontrola nové verze se chová rozdílně v závislosti na platformě firewallu:

- v edici pro systém *Windows* jsou pouze nabídnuty odkazy na bližší informace a stažení instalačního balíku,
- v edicích *Appliance* a *Box* může firewall automaticky stáhnout nový obraz disku a provést aktualizaci celého zařízení.

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.

Pravidelně kontrolovat nové verze

Tato funkce zapíná/vypíná automatickou kontrolu nových verzí. Kontrola se provádí:

- 2 minuty po každém startu *Kerio Control Engine*,
- dále každých 24 hodin.

Výsledek každého pokusu o aktualizaci *Kerio Control* (úspěšného i neúspěšného) je zapsán do záznamu *Debug* (viz kapitola 24.6).

Nabízet ke stažení také betaverze

Při kontrole nových verzí mohou být nabízeny ke stažení a instalaci také betaverze a verze *Release Candidate* produktu *Kerio Control*.

Pokud se chcete podílet na testování betaverzí, zaškrtněte tuto volbu. V případě, že je *Kerio Control* nasazen v ostrém provozu (např. na internetové bráně vaší firmy), nedoporučujeme betaverze instalovat — nezapínejte volbu *Nabízet ke stažení betaverze*.

Odesílat anonymní statistiky...

Odesíláním anonymních statistik můžete pomoci při vývoji produktu Kerio Control. Statistiky neobsahují žádné osobní údaje jako e-mailové adresy, přihlašovací jména nebo hesla.

Stahovat nové verze automaticky

Tato volba je k dispozici pouze v edicích *Appliance* a *Box*. Po jejím zapnutí bude při nalezení nové verze produktu ihned stažen příslušný aktualizační balík a bude možné provést aktualizaci firewallu přímo z administračního rozhraní.

Od poslední kontroly nové verze uplynulo...

V tomto poli se zobrazuje doba, která uplynula od posledního pokusu o aktualizaci *Kerio Control*.

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 24.6) a provést příslušná opatření.

Zkontrolovat

Toto tlačítko spustí okamžitou kontrolu nové verze.

Je-li nalezena nová verze produktu:

- V edici pro systém *Windows* se zobrazí odkaz na stránku s podrobnými informacemi a na stránku pro stažení instalačního balíku.
- V edicích *Appliance* a *Box* se zobrazí tlačítko pro stažení aktualizačního balíku (případně přímo pro zahájení aktualizace, je-li povoleno automatické stahování nových verzí). Aktualizace firewallu trvá nejvýše několik minut. Po jejím dokončení ze zobrazí upozornění, že firewall bude restartován. Po restartu (cca za 1 minutu) bude firewall opět plně funkční.

Podrobnosti o instalaci *Kerio Control* naleznete v kapitole 2.4.

Poznámka:
Je-li k dispozici novější verze produktu, pak se tato informace zobrazuje také jako odkaz na úvodní stránce administračního okna (obrázek s informacemi o aplikaci a licenci). Kliknutím na odkaz se dojde k přepnutí do sekce *Konfigurace → Další volby*, záložka *Aktualizace*.

Kapitola 20

Další nastavení

20.1 Směrovací tabulka

V rozhraní *Kerio Control Administration* lze zobrazit a upravovat systémovou směrovací tabulku firewallu pro protokol IPv4. 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 v systému Windows (*persistent routes* — cesty přidané příkazem `route -p`).

Poznámka:

1. V režimu zálohování internetového připojení (viz kapitola 8.4) 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 8.3) bude zobrazena pouze jedna výchozí cesta, a to přes linku s nejvyšší deklarovanou rychlostí.
3. Protokol IPv6 není podporován.

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 *Kerio Control* trvale udržuje a obnoví ji i po restartu operačního systému.

Typy cest

Ve směrovací tabulce v *Kerio Control* 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*).

- *Cesty pro VPN* — cesty k VPN klientům a do sítí na vzdálených koncích VPN tunelů (podrobnosti viz kapitola 25). 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.

- *Statické cesty* — ručně definované cesty, které udržuje *Kerio Control* (viz níže). Tyto cesty lze přidávat, měnit a odebírat dle potřeby.

  Zaškrtávací pole umožňuje cestu dočasně „vypnout“.

Statické cesty

Kerio Control obsahuje speciální mechanismus pro vytváření a udržování statických cest ve směrovací tabulce. Veškeré statické cesty definované ve *Kerio Control* jsou uloženy do konfiguračního souboru a po každém startu *Kerio Control Engine* vloženy do systémové směrovací tabulky. Po celou dobu běhu *Kerio Control* jsou navíc tyto cesty „hlídány“ — je-li některá z nich odstraněna příkazem `route`, *Kerio Control* ji okamžitě opět přidá.

Poznámka:

1. K implementaci statických cest nejsou využívány trvalé trasy operačního systému (*Kerio Control* 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 8.5.

Definice dynamických a statických cest

Po stisknutí tlačítka *Přidat* (resp. *Změnit* na vybrané cestě) se zobrazí dialog pro definici cesty.

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. *Kerio Control* 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 rozhraní *Kerio Control Administration*).

Odstraňování cest ze směrovací tabulky

Kerio Control umožňuje záznamy ze směrovací tabulky také mazat (tlačítkem *Odebrat*). Pro mazání cest platí následující pravidla:

- Statické cesty jsou plně v režii *Kerio Control*. 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 v rozhraní *Kerio Control Administration* 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.

20.2 Universal Plug-and-Play (UPnP)

Kerio Control 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

Podporu UPnP lze povolit v sekci *Konfigurace* → *Zásady komunikace* → *Bezpečnostní volby*, záložka *Různé*.

Povolit UPnP
: Zapnutí funkce *UPnP*.

Zaznamenat pakety
: Po zapnutí této volby budou do záznamu *Filter* (viz kapitola 24.9) zaznamenány všechny pakety procházející přes porty mapované pomocí UPnP.

Zaznamenat spojení
: Po zapnutí této volby budou do záznamu *Connection* (viz kapitola 24.5) zaznamenána všechna spojení procházející přes porty mapované pomocí UPnP.

Upozornění:

1. Je-li *Kerio Control* provozován na operačním systému *Windows XP*, *Windows Server 2003*, *Windows Vista* nebo *Windows Server 2008*, pak se před zapnutím funkce *UPnP* přesvědčete, 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 *Kerio Control*.
   Poznámka:
   Instalační program *Kerio Control* uvedené služby detekuje a nabízí jejich zastavení a zakázání.

2. 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 firewallu by měl dobře zvážit, zda je důležitější bezpečnost nebo funkčnost aplikací vyžadujících UPnP.
   Pomocí komunikačních pravidel (viz kapitola 9.3) 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 klient	Libovolný	UPnP	Povolit
Zákaz UPnP	Libovolný	Libovolný	UPnP	Zakázat

Obrázek 20.1 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).

20.3 Nastavení serveru odchozí pošty

Kerio Control 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 16.3), při detekci *Peer-to-Peer* sítě (viz kapitola 10.4), při překročení kvóty objemu přenesených dat (viz kapitola 18.1) nebo na základě nastavených výstrah (viz kapitola 21.5).

Pro odeslání e-mailu musí mít *Kerio Control* 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:
Kerio Control neobsahuje žádný vlastní (vestavěný) SMTP server.

Server pro odesílání e-mailových zpráv lze nastavit v sekci *Konfigurace* → *Další volby*, záložka *SMTP server*.

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 *Kerio Control* 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 *Kerio Control* (e-mailové reporty a výstrahy zasílané uživatelům). Nastavení odchozí adresy nemá vliv na zprávy přeposílané při antivirové kontrole (viz kapitola 16.4).
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 v *Kerio Control* vždy zadávat.

Test

Ověření funkčnosti odesílání e-mailových zpráv přes zadaný SMTP server. *Kerio Control* pošle zkušební zprávu na zadanou e-mailovou adresu.

Upozornění:

1. Je-li SMTP server zadán DNS jménem, může být používán až od okamžiku, kdy *Kerio Control* 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.
   Podrobné informace o komunikačních pravidlech naleznete v kapitole 9.

Kapitola 21

Stavové informace

Kerio Control umožňuje správci (popř. jinému oprávněnému uživateli) poměrně detailně sledovat činnost firewallu. V podstatě se jedná o několik druhů informací: sledování stavu, statistiky, e-mailové reporty, statistiky a záznamy.

- Sledovat lze komunikaci jednotlivých počítačů, přihlášené uživatele a spojení, která jsou přes *Kerio Control* navázána.

  Poznámka:

  1. *Kerio Control* 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 9). 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 22.

- Vybrané statistiky mohou být zasílány formou pravidelných denních, týdenních nebo měsíčních reportů.

- 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 *Kerio Control* anglicky (vytváří je přímo *Kerio Control Engine*). Podrobnosti naleznete v kapitole 24.

Jaké informace lze sledovat a jak lze přizpůsobit sledování potřebám uživatele je popsáno v následujících kapitolách.

21.1 Úvodní stránka (dashboard)

Po přihlášení do administračního rozhraní *Kerio Control* se zobrazuje konfigurovatelná úvodní obrazovka (tzv. dashboard), která zobrazuje důležité informace o stavu firewallu a síťové komunikaci. Dashboard je složen z jednotlivých panelů, které lze libovolně přidávat, přesouvat a odebírat. Správce firewallu tak má bez prostředně po přihlášení ty informace, které jej nejvíce zajímají.

Dostupné panely:

- *Vytížení systému* — využití CPU a RAM, zaplnění disku
- *Systém* — základní informace o firewallu a operačním systému
- *Stav systému* — doba od spuštění, informace o dostupných aktualizacích a stavu jednotlivých komponent *Kerio Control*
- *Internetové připojení* — informace o internetových linkách, záložním připojení atd.
- *Nejaktivnější počítače* — počítače stahující a odesílající největší objem dat
- *Informace o VPN* — informace o připojených VPN klientech a VPN tunelech
- *Licence* — podrobné informace o licenci produktu
- *Graf síťové komunikace* — graf vybraného typu (viz sekce 22.2). Na obrazovku Dashboard lze přidat libovolný počet grafů.

21.2 Aktivní počítače a přihlášení uživatelé

V sekci *Stav* → *Aktivní počítače* se zobrazují počítače z lokální sítě, případně přihlášení uživatelé, kteří komunikují přes *Kerio Control* do Internetu.

Poznámka:
Podrobnosti o přihlašování uživatelů na firewall naleznete v kapitole 13.1.

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.

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 *Kerio Control* 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 14.1).

Počáteční čas
Datum a čas, kdy byl daný počítač poprvé zaregistrován *Kerio Control*. Tato informace se udržuje v operační paměti pouze po dobu běhu *Kerio Control 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 v *Kerio Control*, na němž se ověřil,
- *NTLM* — uživatel byl automaticky ověřen v NT doméně pomocí NTLM (funguje při použití WWW prohlížeče *Internet Explorer* nebo *Firefox/SeaMonkey*),
- *VPN klient* — uživatel se připojil do lokální sítě pomocí aplikace *Kerio VPN Client* (podrobnosti viz kapitola 25).
  Poznámka:
  Pro VPN klienty se nezobrazují spojení a neměří se objem přenesených dat.

Detaily o přihlašování a ověřování uživatelů naleznete v kapitole 13.1.

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:

Uživatelská kvóta
Tato volba zobrazí informace o kvótě příslušného uživatele (rozhraní *Kerio Control Administration* 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.

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.

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.

- *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). *Kerio Control* 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:
Kerio Control nerozpoznává konkrétní *P2P* síť, pouze na základě určitých testů vyhodnotí, že klient je pravděpodobně do takové sítě připojen. Podrobnosti naleznete v kapitole 10.4.

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 uživatelských statistikách (viz kapitola 23).
- *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.

Zobrazované informace o spojení:

Komunikační pravidlo

Název komunikačního pravidla *Kerio Control* (viz kapitola 9), 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).

Pravidlo pro řízení šířky pásma
Pravidlo pro omezení nebo rezervaci šířky pásma, které bylo aplikováno na toto spojení (prázdný sloupec — nebylo aplikováno žádné pravidlo).

Rozložení zátěže
Pracuje-li firewall v režimu rozložení zátěže, je zde (v případě spojení do/z Internetu) uvedeno rozhraní, přes které je spojení směrováno.

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 *Kerio Control*.
S každým novým paketem v rámci tohoto spojení je časový limit nastaven na výchozí hodnotu. Nejsou-li spojením přenášena žádná data, *Kerio Control* 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 21.3). Spojení mezi počítači v lokální síti *Kerio Control* 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*).

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 prohlížeče.

21.3 Zobrazení síťových spojení

V sekci *Stav* → *Spojení* lze sledovat veškerá síťová spojení, která dokáže *Kerio Control* zachytit, tzn.:

- spojení navázaná klienty přes *Kerio Control* do Internetu
- spojení navázaná z počítače, na němž *Kerio Control* 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 firewallu může vybrané spojení „násilně“ ukončit.

Poznámka:

1. *Kerio Control* nezachytí (a tudíž nezobrazí) spojení navázaná mezi lokálními klienty.
2. Protokol UDP je tzv. nespojovaný protokol — nenavazuje žádné spojení, komunikace probíhá formou jednotlivých zpráv (tzv. datagramů). V tomto případě jsou sledována tzv. pseudospojení (periodická výměna zpráv mezi dvěma počítači je považována za jedno spojení).

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). Řádky jsou barevně zvýrazněny: zelená barva — odchozí spojení, červená barva — příchozí spojení.

Sloupce zobrazují následující informace:

Komunikační pravidlo
Název komunikačního pravidla, kterým bylo povoleno navázání příslušného spojení (viz kapitola 9).

Služba
Název služby, která je tímto spojením přenášena (je-li taková služba v *Kerio Control* definována — viz kapitola 17.3). Pokud *Kerio Control* danou službu nezná, zobrazí se číslo portu a protokol (např.
5004/UDP).

Zdroj, Cíl
IP adresa zdroje (iniciátora spojení) a cíle.

Pravidlo pro řízení šířky pásma
Pravidlo pro omezení nebo rezervaci šířky pásma, které bylo aplikováno na toto spojení (prázdný sloupec — nebylo aplikováno žádné pravidlo).

Rozložení zátěže
Pracuje-li firewall v režimu rozložení zátěže internetového připojení (viz kapitola 8.3), je zde v případě spojení do/z Internetu uvedeno rozhraní, přes které je spojení směrováno.

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.

Stáří
Celková doba, po kterou je spojení navázáno.

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).

Typ
Rozlišení směru spojení — odchozí nebo příchozí.

Informace v okně *Spojení* mohou být 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 *Kerio Control*.

  Tuto volbu lze využít pro zvýšení přehlednosti (pokud nás zajímají pouze spojení mezi počítači v lokální síti a Internetem).

- *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:

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.

Nastavení barev

Tlačítko *Barvy* slouží k nastavení barev, kterými budou jednotlivá spojení zobrazována:

V každé položce je možné vybrat barvu nebo hodnotu *Výchozí*. Ta představuje barvu nastavenou v operačním systému (zpravidla černá pro text a bílá pro pozadí).

Barva písma

- *Aktivní spojení* — spojení, jimiž jsou aktuálně přenášena data
- *Neaktivní spojení* — TCP spojení, která byla ukončena, ale jsou dosud udržována (standard stanoví, že spojení musí být udržováno ještě 2 minuty po jeho ukončení — z důvodu opakovaného vysílání chybných paketů)

Barva pozadí

- *Lokální spojení* — spojení, jejichž zdrojem nebo cílem je některá z IP adres počítače s *Kerio Control*
- *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 9.

21.4 Přehled připojených VPN klientů

V sekci *Stav* → *VPN klienti* lze získat přehled o VPN klientech aktuálně připojených k VPN serveru v *Kerio Control*.

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 *Kerio Control* 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).
- IP adresa — veřejná IP adresa počítače, ze kterého se klient připojuje (viz výše — sloupec *Jméno počítače*).
- Stav klienta — *připojuje se*, *ověřuje se* (*Kerio Control* ověřuje 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.

21.5 Výstrahy

Kerio Control může automaticky informovat správce o důležitých událostech, které zpracovával nebo zachytil. Díky tomuto mechanismu není nutné se pravidelně přihlašovat k firewallu a kontrolovat všechny stavové informace a záznamy (občasná kontrola však rozhodně není na škodu!).

Kerio Control generuje výstrahu vždy při zachycení některé ze sledovaných událostí. Všechny tyto výstrahy se zapisují do záznamu *Alert* (viz kapitola 24.3). Správce firewallu 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 v *Kerio Control* nastaven server odchozí pošty (viz kapitola 20.3).

Nastavení výstrah

Zasílání výstrah na vybrané události lze nastavit v sekci *Konfigurace* → *Statistiky a výstrahy*, záložka *Nastavení výstrah*.

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 16).
- *Selhání antivirové kontroly* — antivirovému modulu se z určitého důvodu nepodařilo zkontrolovat soubor (typicky archiv chráněný heslem nebo poškozený soubor).
- *Dosaženo limitu počtu spojení na jeden počítač* — některý počítač v lokální síti má otevřen maximální povolený počet spojení (viz kapitola 10.3). 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 *Kerio Control* nainstalován, zbývá již velmi málo místa (méně než 11% kapacity disku).
  Kerio Control potřebuje diskový prostor pro ukládání záznamů, statistik, konfigurace, dočasných souborů (např. stažený instalační archiv nové verze nebo soubor, který je právě kontrolován antivirem) a dalších informací. Obdrží-li správce *Kerio Control* toto upozornění, měl by neprodleně provést příslušná opatření (uvolnění místa na disku, výměna disku za větší apod.)
- *Nová verze Kerio Control ke stažení* — modul automatické kontroly nových verzí nalezl na serveru firmy Kerio Technologies novější verzi *Kerio Control*.

- *Překročena uživatelská kvóta objemu přenesených dat* — některý uživatel překročil nastavený denní, týdenní nebo měsíční limit objemu přenesených dat a *Kerio Control* provedl příslušnou akci. Podrobnosti viz kapitola 18.1.
- *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 8.4.
- *Vypršení licence* — blíží se datum skončení platnosti licence nebo Software Maintenance *Kerio Control* nebo některého z integrovaných modulů (*Kerio Control Web Filter*, antivirus *Sophos*). Správce by měl zkontrolovat data vypršení a obnovit příslušnou licenci nebo Software Maintenance (podrobnosti viz kapitola 5).
- *Vytočení / zavěšení RAS linky* — *Kerio Control* vytáčí, resp. zavěšuje některou z RAS linek (viz kapitola 7). 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 *Kerio Control*) 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 17.2).

Šablony výstrah

Formát zpráv zasílaných uživatelům (e-mailem nebo SMS) a zobrazovaných v administračním rozhraní (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 *Kerio Control* při odesílání zprávy dosadí konkrétní hodnoty. Správce firewallu může šablony libovolně upravovat a přizpůsobit tak podobu jednotlivých zpráv dle potřeby a vkusu.

Jednotlivé šablony jsou uloženy v podadresáři `templates` instalačního adresáře *Kerio Control*:

- podadresář `console` — zprávy zobrazované v levé části sekce *Stav* → *Výstrahy* (přehled),
- podadresář `console\details` — zprávy zobrazované v pravé 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.

Každý podadresář obsahuje sadu šablon ve všech jazycích, které *Kerio Control* podporuje. V rozhraní *Kerio Control Administration* se výstrahy zobrazují v aktuálně nastaveném jazyce. E-mailové a SMS výstrahy jsou zasílány vždy v angličtině.

Zobrazení výstrah v administračním rozhraní

Sekce *Stav* → *Výstrahy* zobrazuje všechny výstrahy, které *Kerio Control* odeslal uživatelům od svého spuštění . Výstrahy jsou zobrazovány v jazyce *Administration Console*.

Poznámka:
Zasílání jednotlivých výstrah e-mailem je potřeba nastatit v sekci *Konfigurace* → *Statistiky a výstrahy*, záložka *Výstrahy* (viz výše).

V levé části sekce *Výstrahy* je uveden seznam všech dosud odeslaných výstrah (seřazený podle dat a časů, kdy jednotlivé události nastaly).

Na každém řádku je zobrazena jedna výstraha:

- *Datum* — datum a čas, kdy nastala příslušná událost,
- *Výstraha* — typ zachycené události.

Po kliknutí na vybranou výstrahu se v pravé části sekce *Výstrahy* zobrazí podrobné informace o příslušné události včetně textového popisu (dle šablon v adresáři `console\details` — viz výše).

Poznámka:
Podrobnosti o vybrané události lze volitelně skrýt nebo zobrazit tlačítkem v pravém dolním rohu okna (ve výchozím nastavení jsou podrobnosti zobrazeny).

Záznam Alert

Záznam *Alert* obsahuje informace o všech výstrahách, které *Kerio Control* vygeneroval (bez ohledu na to, zda byly zaslány správci/uživateli e-mailem či nikoliv). Podrobnosti viz kapitola 24.3.

21.6 Stav systému (edice Appliance a Box)

Sekce *Stav systému* zobrazuje aktuální využití procesoru (CPU), operační paměti (RAM) a diskového prostoru počítače, resp. zařízení, na kterém je provozována aplikace *Kerio Control*.

Časový interval
: Výběr časového období, ve kterém bude zobrazen průběh zatížení CPU a využití RAM (2 hodiny nebo 1 den).

CPU
: Časový průběh zatížení CPU počítače (zařízení). Nárazové krátkodobé zatížení („špičky“ v grafu) je normální jev, způsobený např. síťovou aktivitou.

RAM
: Časový průběh využití operační paměti (RAM).

Diskový prostor
: Aktuální obsazený a volný prostor na pevném disku, resp. paměťové kartě.

Úlohy
: Restart systému nebo vypnutí zařízení (k dispozici pouze v edicích *Appliance* a *Box*).

Nedostatek systémových prostředků může vážným způsobem ohrozit chod aplikace *Kerio Control*. Při trvale vysokém zatížení CPU a/nebo nedostatku paměti RAM doporučujeme zkontrolovat, jaké další aplikace a služby jsou na systému spuštěny. V případě edic *Appliance* a *Box* je vhodné *Kerio Control* restartovat a poté opět zkontrolovat využití systémových prostředků.

Při nedostatku volného místa na disku je možné tlačítkem *Spravovat* smazat některé soubory vytvářené za běhu *Kerio Control* (záznamy, statistická data atd.) a nastavit limity, které zabrání vyčerpání volného místa na disku.

Správa diskového prostoru

Dostatek volného místa na disku můžeme zajistit těmito způsoby:

- Uvolnit místo na disku smazáním starých či nepotřebných souborů (záznamy, statistická data atd.),
- Nastavit limity velikostí souborů vytvářených aplikací *Kerio Control* tak, aby nedocházelo k vyčerpání volného místa na disku.

V dialogu jsou zobrazeny pouze ty komponenty, jejichž data zabírají na disku určité místo (řádově MB).

Kapitola 22

Základní statistiky

Kerio můžeme sledovat statistické informace o uživatelích (objem přenesených dat, používané služby, kategorizace navštívených WWW stránek) a síťových rozhraních firewallu s *Kerio Control* (objem přenesených dat, zatížení linek).

V rozhraní *Kerio Control Administration* 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 v uživatelském WWW rozhraní firewallu (viz kapitola 23).

22.1 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 18.1). 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 23.2).

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 (směr *IN* znamená data přijatá tímto uživatelem, směr *OUT* data vyslaná tímto uživatelem).
2. Údaje o přeneseném objemu dat jednotlivých uživatelů jsou ukládány do souboru `stats.cfg` v adresáři aplikace *Kerio Control*. Při ukončení a novém spuštění *Kerio Control 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:

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 18.1). 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 podnabídku 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.

22.2 Grafy síťové komunikace

V sekci *Stav* → *Statistiky*, záložka *Statistiky rozhraní* lze podrobně sledovat objem dat přenesených přes jednotlivá rozhraní firewallu 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).

Příklad
Firewall 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 *Kerio Control*. Při ukončení a novém spuštění *Kerio Control 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:

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.

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).

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*).

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 23

Statistiky využívání Internetu a reporty

Kerio Control poskytuje podrobné statistické informace o aktivitě uživatelů, objemu přenesených dat, navštívených WWW stránkách a kategoriích stránek. Tyto informace lze využít např. pro sledování pracovního a nepracovního využívání Internetu jednotlivými uživateli.

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 statistik a reportů je jejich snadná dostupnost. Uživatel (typicky vedoucí pracovník) si může statistiky prohlížet ve webovém prohlížeči a/nebo si nechat zasílat pravidelné e-mailové reporty.

Tato kapitola se zabývá nastavením statistik v administraci *Kerio Control*. Webové rozhraní se statistikami je podrobně popsáno v manuálu *Kerio Control — Příručka uživatele*.

Poznámky:

1. Správce firewallu by měl informovat uživatele o tom, že jejich aktivita je sledována.
2. Statistiky a reporty aplikace *Kerio Control* mají informativní charakter. Nedoporučujeme je používat např. pro přesné rozúčtování nákladů na internetové připojení na jednotlivé uživatele.

23.1 Sledování a ukládání statistických dat

Pro sledování výše popsaných statistik musí *Kerio Control* získávat data různého typu. Tato data se uchovávají v tzv. hlavní databázi. Celkovou dobu, pro kterou *Kerio Control* statistiky uchovává, lze nastavit v sekci *Statistiky a výstrahy* (viz kapitola 23.2). Výchozí nastavení je *24 měsíců* (tj. 2 roky).

Kerio Control Engine z technických důvodů uchovává získaná statistická data ve své vyrovnávací paměti (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 *Kerio Control 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 13.

- 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 9.8).

  V případě zabezpečené komunikace (protokol HTTPS) není možné sledovat navštívené stránky, pouze objem přenesených dat.

  Při použití proxy serveru v *Kerio Control* sleduje navštěvované stránky přímo proxy server (viz kapitola 11.5).

- Pro sledování kategorií navštívených WWW stránek musí být také aktivní modul *Kerio Control 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 15.3.

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 9.3) 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 18.2 a 12.3).

23.2 Nastavení statistik, reportů a kvóty

Sledování statistik může za určitých okolností (vysoký počet uživatelů, velký objem přenášených dat, nízký výkon počítače s *Kerio Control* apod.) zpomalovat činnost firewallu a rychlost internetového připojení. *Kerio Control* 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 a diskový prostor firewallu.

Nastavení statistik rovněž ovlivňují sledování uživatelské kvóty objemu přenesených dat (viz kapitoly 18.1 a 22).

V sekci *Konfigurace* → *Statistiky a výstrahy*, záložka *Sledování dat*, lze nastavit sledování statistik, účtovací období a zasílání reportů e-mailem.

Sledování statistik

Volba *Statistiky využívání Internetu* zapíná/vypíná sledování všech statistik (resp. sběru dat, ze kterých se statistiky vytvářejí).

Volba *Sledovat aktivitu 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 *Mazat statistiky starší než...* 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.

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 18.2.

Pravidelný report

Kerio Control umožňuje zasílat statistiky formou e-mailových zpráv.

Zasílání reportů se nastavuje pomocí pravidel. Každé pravidlo definuje jednoho příjemce reportu. Příjemce může být uživatel Kerio Control (musí však mít definovanou e-mailovou adresu) nebo libovolná e-mailová adresa. Volitelně lze zasílat denní, týdenní a měsíční reporty.

Uživatelům Kerio Control budou reporty zasílány v jejich preferovaném jazyce, na externí e-mailové adresy budou odesílány ve *Výchozím jazyce*.

Poznámka: Pro zasílání reportů e-mailem je potřeba správně nastavit server odchozí pošty v sekci *Konfigurace* → *Další volby* → *SMTP server*.

Výjimky pro sledování statistik

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.

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 17.2.
- *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 17.1.
- *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 18.
- *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 17.4).

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 17.1.
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.

Přístup ke statistikám

Nastavení přístupu uživatelů ke statistikám využívání Internetu a zasílání pravidelných e-mailových reportů dle požadavků.

Vzhled

Upřesňující nastavení formátu statistik a e-mailových reportů:

- Formát jména uživatele.
- Výchozí jazyk e-mailových reportů — pro reporty zasílané na externí e-mailové adresy.

Přístupová práva a e-mailové reporty

Přístup ke statistikám a zasílání reportů se nastavuje pomocí jednoduchých pravidel. Pravidel lze přidat libovolný počet a na jejich pořadí nezáleží.
Definice pravidla:

- Uživatel — lze vybrat libovolný počet uživatelů a/nebo skupin z interní databáze Kerio Control a/nebo mapovaných adresářových služeb.
  Uživatelům Kerio Control se reporty zasílají na e-mailovou adresu definovanou v uživatelském účtu. Zároveň si mohou prohlížet statistiky online we webovém rozhraní Kerio Control.
- E-mailová adresa — libovolná e-mailová adresa, na kterou budou zasílány e-mailové reporty. E-mailovou adresu nelze využít pro přístup ke statistikám online. Pro zasílání reportů na více adres definujte více samostatných pravidel.
- Data — statistiky obsažené v reportech a/nebo přístupné online. Je možné zahrnout statistiky všech uživatelů, nebo pouze vybraných uživatelů a skupin (např. podřízení nebudou mít přístup ke statistikám svých nadřízených).
- Pravidelné reporty — automatické zasílání e-mailových reportů dle nastavených podmínek (denně, týdně, měsíčně).

Pro zasílání e-mailových zpráv musí být správně nastaven server odchozí pošty (*Konfigurace → Další volby → SMTP server*).
Tlačítkem *Znovu odeslat* je možné znovu zaslat aktuální e-mailové reporty, pokud z nějakého důvodu nebyly doručeny.

Přístup uživatelů

Hromadné nastavení pro všechny uživatele Kerio Control:

- Povolení prohlížení svých vlastních statistik ve webovém rozhraní Kerio Control,
- Automatické zasílání e-mailových reportů (denně, týdně, měsíčně).

23.3 Přihlášení do webového rozhraní a zobrazení statistik

K prohlížení statistik je třeba se přihlásit do WWW rozhraní *Kerio Control*. Uživatel (resp. skupina, do které je zařazen) musí mít právo prohlížet statistiky — viz kapitola 23.2. WWW rozhraní lze otevřít několika způsoby v závislosti na tom, zda se chceme přihlásit přímo z počítače, na kterém je *Kerio Control* nainstalován (lokální přístup) nebo z jiného počítače (vzdálený přístup).

Poznámka:
Podrobnosti o WWW rozhraní *Kerio Control* viz kapitola 14.2.

Přístup ke statistikám z počítače s Kerio Control (Windows)

Na počítači, kde je *Kerio Control* nainstalován, můžeme webové rozhraní se statistikami otevřít:

- Odkazem *Internet Usage Statistics* z kontextového menu programu *Kerio Control Engine Monitor* (ikona v oznamovací oblasti nástrojové lišty — viz kapitola 3.1).
- Odkazem *Internet Usage Statistics* v menu *Start* → *Programy* → *Kerio* → *Kerio Control*.

Oba tyto odkazy otevírají nezabezpečené webové rozhraní na lokálním počítači (`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 *Kerio Control* a portům WWW rozhraní je možné přistupovat ke statistikám těmito způsoby:

- Pokud jsme aktuálně přihlášení ke správě *Kerio Control*, pak můžeme v sekci *Stav* → *Statistiky* použít odkaz *Statistiky využívání Internetu* v zápatí stránky. Tento odkaz otevře zabezpečené webové rozhraní ve výchozím WWW prohlížeči.

  Poznámka:
  URL pro tento odkaz je vytvořeno ze jména serveru a portu zabezpečeného WWW rozhraní (viz kapitola 14.1). Tím je zaručena funkčnost tohoto odkazu z počítače s *Kerio Control* a z lokální sítě. Má-li odkaz *Statistiky využívání Internetu* funkční i při

vzdálené správě přes Internet, musí být příslušné jméno serveru uvedené ve veřejném DNS (s příslušnou veřejnou IP adresou firewallu) a komunikační pravidla musí povolovat přístup k portu zabezpečeného WWW rozhraní (`4081` — předdefinovaná služba *Kerio Control WebAdmin*).

- Na adrese `https://server:4081/star` nebo `http://server:4080/star`. Toto je URL určené výhradně pro přístup ke statistikám. 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 *Kerio Control*. Pokud má uživatel právo prohlížet statistiky, zobrazí se úvodní stránka s celkovými statistikami (viz níže), případně jeho vlastními statistikami. 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 statistických dat

Webové rozhraní je primárně určeno k prohlížení statistik a přehledů za určité období. Při sledování a vyhodnocování informací pro statistiky musí *Kerio Control* zpracovat poměrně velké množství dat. Aby nedocházelo k příliš velkému zatěžování firewallu, aktualizují se data pro statistiky vždy cca 1x za hodinu. V pravém horním rohu každé stránky webového rozhraní je vždy uvedena informace o tom, kdy proběhla poslední aktualizace těchto dat.

Z těchto důvodů nejsou statistiky vhodné pro sledování aktivity uživatelů v reálném čase. Pro tyto účely doporučujeme použít sekci *Aktivní počítače* v rozhraní *Kerio Control Administration* (viz kapitola 21.2).

Kapitola 24

Záznamy

Záznamy uchovávají zprávy o vybraných událostech, k nimž v *Kerio Control* došlo, nebo které *Kerio Control* 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 *Kerio Control* 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 rozhraní *Kerio Control Administration*.

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.

Kerio Control 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.

24.1 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 ze záznamu do schránky. Kopírování textu volbou z kontextového menu je možné pouze v prohlížeči *Internet Explorer*, kde je však navíc nutné povolit přístup ke schránce.

[7] Lokálním diskem se rozumí disk počítače, na kterém je *Kerio Control* nainstalován, nikoliv disk počítače, ze kterého jej spravujeme!

Pro kopírování textu do schránky doporučujeme používat klávesovou zkratku `Ctrl+C` (resp. `Apple+C` na počítačích Mac). Tento způsob funguje ve všech podporovaných prohlížečích.

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 *Kerio Control* nainstalován. Záznamy lze ukládat i v případě vzdálené správy *Kerio Control*.

Volba *Uložit záznam* otevírá dialog pro nastavení volitelných parametrů:

- *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.

Zvýrazňování

Nastavení barevného zvýraznění řádků záznamu vyhovujících určitým podmínkám (podrobnosti viz níže).

Nastavení záznamu

Dialog pro nastavení záznamu do souboru, rotace záznamu a odesílání zpráv na *Syslog*. Podrobnosti viz kapitola 24.2.

Smazat záznam

Smazání celého záznamu. Tato volba nenávratně smaže všechny informace ze záznamu (nikoliv pouze část zobrazenou v aktuálním okně).

> ***Upozornění:***
> Smazaný záznam již nelze obnovit!

Poznámka:
Měnit nastavení záznamu a mazat záznam může pouze uživatel s přístupem ke správě 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.

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.

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. *Kerio Control* 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/

24.2 Nastavení záznamů

Volba*Nastavení záznamu* v kontextovém menu záznamu umožňuje nastavit volby pro uchovávání záznamu a odesílání zpráv na server *Syslog*. Tyto parametry se nastavují odděleně pro každý záznam.

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. Soubor má jméno shodné s názvem záznamu a příponou `.log`. Pokud je povolena rotace záznamů, pak se starší záznamy ukládají do souborů s názvy odvozenými od data a času rotace.

Všechny soubory záznamů se ukládají do podadresáře `logs` „hlavního“ adresáře aplikace *Kerio Control*, tj.:

- v edici pro systém *Windows* typicky:

  `C:\Program Files\Kerio\WinRoute\Firewall\logs`

- v edicích *Appliance* a *Box* vždy:

  `/opt/kerio/winroute/logs`

Poznámka:
Nebude-li záznam ukládán do souboru na disku, pak budou v záznamu zobrazovány pouze zprávy vygenerované od posledního přihlášení ke *Kerio Control Engine*. Po odhlášení (resp. uzavření okna s administračním rozhraním) budou tyto zprávy ztraceny.

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.

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 23.2). Rotace probíhá vždy podle výše uvedených pravidel.

Nastavení záznamu na Syslog server

Záložka *Externí záznam* umožňuje nastavit odesílání jednotlivých zpráv, které jsou zapisovány do daného záznamu, na *Syslog* server. Stačí zadat pouze DNS jméno nebo IP adresu *Syslog* serveru.

Služba *Syslog* rozlišuje záznamy podle typu (*Facility*) a důležitosti (*Severity*). Tyto hodnoty jsou pevně nastavené pro každý záznam (v záložce *Externí záznam* lze zjistit aktuální hodnoty pro daný záznam).

V aplikaci *Kerio Control* je typ záznamu (*Facility*) pro všechny záznamy nastaven na hodnotu *16: Local use 0*. Přehled hodnot *Severity* je uveden v tabulce 24.1.

Záznam	Důležitost (Severity)
Alert	1: Alert
Config	6: Informational
Connection	6: Informational
Debug	7: Debug
Dial	5: Notice
Error	3: Error
Filter	6: Informational
Http	6: Informational
Security	5: Notice
Sslvpn	5: Notice
Warning	4: Warning
Web	6: Informational

Tabulka 24.1 Důležitost (Severity) záznamů produktu Kerio Control

24.3 Záznam Alert

Záznam *Alert* obsahuje informace o všech výstrahách, které *Kerio Control* 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 výstrahy* 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 21.5).

24.4 Záznam Config

Záznam *Config* uchovává kompletní historii komunikace administračního rozhraní s *Kerio Control 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 Kerio Control*

   Příklad
   ```
   [18/Apr/2011 10:25:02] standa - session opened
   for host 192.168.32.100
   [18/Apr/2011 10:32:56] standa - session closed
   for host 192.168.32.100
   ```

   - `[18/Apr/2011 10:25:02]` — datum a čas, kdy byl záznam zapsán
   - `standa` — jméno uživatele přihlášeného ke správě *Kerio Control*
   - `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 uzavření okna prohlížeče s administračním rozhraním).

2. *Změny v konfigurační databázi*

   Jedná se o změny provedené uživatelem v administračním rozhraní. Pro komunikaci s databází se používá zjednodušená forma jazyka SQL.

   Příklad
   ```
   [18/Apr/2011 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/2011 10:27:46]` — datum a čas, kdy byl záznam zapsán
   - `standa` — jméno uživatele přihlášeného ke správě *Kerio Control*
   - `insert StaticRoutes ...` — vložení záznamu do konfigurační databáze *Kerio Control* (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* → →*Zásady komunikace* → *Komunikační pravidla* se do záznamu *Config* vypíše kompletní seznam aktuálních komunikačních pravidel.

Příklad
```
[18/Apr/2011 12:06:03] Admin - New traffic policy set:
[18/Apr/2011 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/2011 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 9.1) má namísto čísla označení `default`.

24.5 Záznam Connection

Záznam *Connection* obsahuje informace o spojeních odpovídajících komunikačním pravidlům se zapnutou volbou *Zaznamenat odpovídající spojení* (viz kapitola 9) nebo splňujících určité podmínky (např. záznam *UPnP* komunikace — viz kapitola 20.2). Dále se zaznamenávají informace o všech spojeních nad protokolem IPv6.

Jak číst záznam Connection?

```
[18/Apr/2011 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/2011 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 v *Kerio Control*.
- `[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 v *Kerio Control* příslušná služba definována (viz kapitola 17.3), 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 11.1) 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 *Kerio Control*).

- `[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).

24.6 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 *Kerio Control*. 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 24.1) další volby umožňující podrobné nastavení záznamu nebo jednorázové zobrazení stavových informací.

Tyto volby jsou k dispozici pouze uživatelům s plným přístupem ke správě *Kerio Control* (tj. přístupem pro čtení i zápis — viz kapitola 18.1).

Formát zaznamenávaných paketů

Při záznamu síťové komunikace se používá šablona, která určuje, jaké informace mají být zaznamenány a v jakém formátu. Tím lze záznam zpřehlednit a zmenšit nároky na diskový prostor.
Podrobná nápověda je k dispozici přímo v okně pro zápis šablony.

IP komunikace

Sledování paketů IPv4 nebo IPv6 na základě zadaného výrazu.

Výraz je potřeba 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 *Kerio Control*. 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 *Kerio Control*. Tyto informace mohou být užitečné při řešení problémů s komponentami *Kerio Control* 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 *Kerio Control* (antivirová kontrola, kategorizace WWW stránek, detekce a eliminace *P2P* sítí, detekce a prevence útoků, zahozené pakety atd.),
- *Accounting* — ověřování uživatelů a sledování jejich aktivity (rozpoznávání protokolů, statistiky a reportování atd.),
- *Kerio Control services* — protokoly zpracovávané službami *Kerio Control* (*DHCP server*, modul *DNS*, WWW rozhraní a podpora protokolu *UPnP*, ohlašování směrovače IPv6),
- *Decoded protocols* — zobrazení obsahu zpráv vybraných protokolů (*HTTP* a *DNS*),
- *Miscellaneous* — různé další informace (např. zpracování paketů modulem *Řízení šířky pásma*, přepínání primárního a záložního internetového připojení, HTTP cache, využití licence, kontrola aktualizací, spolupráce s dynamickým DNS, systémová konfigurace v edicích *Appliance* a *Box* atd.),
- *Protocol inspection* — zprávy od jednotlivých inspekčních modulů *Kerio Control* (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* atd.).

24.7 Záznam Dial

Záznam o vytáčení, zavěšování a době připojení vytáčených linek.

V záznamu *Dial* se objevují zprávy několika různých typů:

1. Ruční vytočení linky (v rozhraní *Kerio Control Administration* — viz kapitola 7 nebo přímo v operačním systému)

   ```
   [15/Mar/2011 15:09:27] Line "Pripojeni" dialing,
   ```

```
console 127.0.0.1 - Admin
```

```
[15/Mar/2011 15:09:39] Line "Pripojeni" successfully connected
```

První záznam je zapsán v okamžiku zahájení vytáčení. Záznam vždy obsahuje jméno vytáčené linky v *Kerio Control* (viz kapitola 7). Pokud byla linka vytočena z administračního rozhraní, obsahuje navíc tyto informace:

- odkud byla linka vytočena (`console` — administrační rozhraní, `system` — operační systém),
- IP adresu klienta (tj. počítače, ze kterého je prováděna správa),
- 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/2011 15:29:18] Line "Pripojeni" hang-up,
console 127.0.0.1 - Admin
```

```
[15/Mar/2011 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/2011 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/2011 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/2011 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 — pouze v edici pro systém *Windows*)

   ```
   [15/Mar/2011 15:53:42] Packet
   TCP 192.168.1.3:8580 -> 212.20.100.40:80
   initiated dialing of line "Pripojeni"

   [15/Mar/2011 15:53:53] Line "Pripojeni" successfully connected
   ```

   První záznam je zapsán v okamžiku, kdy *Kerio Control* 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/2011 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/2011 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.

24.8 Záznam Error

Záznam *Error* zobrazuje závažné chyby, které mají zpravidla vliv na chod celého firewallu. Správce *Kerio Control* 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.

Formát záznamů v okně Error
`[15/Apr/2011 15:00:51] (6) Automatic update error: Update failed.`

- `[15/Apr/2011 15:00:51]` — časová značka (datum a přesný čas, kdy k chybě došlo),
- `(6)` — související systémový chybový kód (pouze u některých chyb),
- `Automatic update error: Update failed.` — popis chyby (v tomto případě selhání automatické aktualizace produktu).

Kategorie chybových hlášení vypisovaných do záznamu *Error*:

- Problémy se systémovými zdroji (nedostatek paměti, chyba alokace paměti atd.),
- Problémy s licencí (licence vypršela, licence brzy vyprší, nesprávná licence atd.),
- Interní chyby (nelze přečíst směrovací tabulku, IP adresy rozhraní apod.),
- Problémy s licencí (překročen maximální počet uživatelů, nelze najít soubor s licencí, vypršení Software Maintenance atd.),
- Cchyby konfigurace (nelze načíst konfigurační soubor, detekována smyčka v nastavení modulu *DNS* nebo *Proxy serveru* apod.),
- Síťové (socketové) chyby,
- Cchyby při spouštění a zastavování *Kerio Control Engine* (problémy s nízkoúrovňovým ovladačem, inicializací používaných systémových knihoven a služeb, konfigurační databází atd.),
- Chyby souborového systému (nelze otevřít / uložit / smazat soubor),
- Chyby SSL (problémy s klíči, certifikáty atd.),
- Chyby modulu *Kerio Control Web Filter* (nelze aktivovat licenci apod.),
- Chyby *Kerio VPN*,

- Chyby HTTP cache (chyby při čtení / ukládání souborů, nedostatek volného místa na disku apod.),
- Chyby modulu *Kerio Control Web Filter*,
- Chyby ověřovacího subsystému,
- Chyby antivirového modulu (test antiviru proběhl neúspěšně, problém s ukládáním dočasných souborů atd.),
- Chyby telefonického připojení (nelze načíst definovaná připojení, chyba konfigurace linky atd.),
- Chyby LDAP (nelze najít server, neúspěšné přihlášení atd.),
- Chyby automatické aktualizace a registrace produktu,
- Chyby dynamického DNS (nelze se připojit k serveru, nelze aktualizovat záznam atd.),
- Chyby modulu *Řízení šířky pásma*,
- Chyby WWW rozhraní,
- Výpisy paměti po pádu aplikace,
- Chyby NTP klienta (synchronizace času se serverem),
- Chyby webového rozhraní *Kerio Control Administration*,
- Chyby systému prevence útoků.

Poznámka:
Je-li v záznamu *Error* opakovaně hlášena chyba, kterou nedokážete svépomocí odstranit (resp. ani zjistit její příčinu), kontaktujte technickou podporu firmy Kerio Technologies.

24.9 Záznam Filter

Záznam o WWW stránkách a objektech blokovaných, resp. povolených HTTP a FTP filtrem (viz kapitoly 15.2 a 15.5) a o paketech vyhovujících komunikačním pravidlům se zapnutou volbou *Zaznamenat odpovídající pakety* (viz kapitola 9) nebo jiným podmínkám (např. záznam *UPnP* komunikace — viz kapitola 20.2).

Každý řádek tohoto záznamu obsahuje:

- Jedná-li se o pravidlo pro HTTP nebo FTP: název pravidla, uživatel a IP adresa počítače, který požadavek vyslal a přesné URL objektu.
- Jedná-li se o komunikační pravidlo: detailní informace o zachyceném paketu (zdrojová a cílová adresa, porty, velikost atd.). Formát zaznamenávaných paketů je dán

šablonou, kterou lze upravit příslušnou volbou v kontextovém menu záznamu *Filter*. Podrobná nápověda je k dispozici přímo v okně pro zápis šablony.

Příklad záznamu pro HTTP pravidlo

```
[18/Apr/2011 13:39:45] ALLOW URL 'Sophos update'
192.168.64.142 standa HTTP GET
http://update.kerio.com/antivirus/datfiles/4.x/dat-4258.zip
```

- `[18/Apr/2011 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)
- `'Sophos 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/2011 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/2011 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 7)
- `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

24.10 Záznam Http

Kompletní záznam HTTP požadavků, které byly zpracovány inspekčním modulem protokolu HTTP (viz kapitola 17.3) nebo vestavěným proxy serverem (viz kapitola 11.5).

Záznam *Http* může mít standardní formát logu WWW serveru *Apache* (viz http://www.apache.org/) nebo formát logu proxy serveru *Squid* (viz http://www.squid-cache.org/). Formát záznamu lze nastavit v kontextovém menu. Změna formátu bude aplikována na nově zapsané zprávy (stávající zprávy již nelze přeformátovat).

Poznámka:

1. Do tohoto záznamu se ukládají pouze přístupy na povolené stránky. Požadavky blokované HTTP pravidly lze sledovat v záznamu *Filter* (viz kapitola 24.9), je-li v příslušném pravidle zapnuta volba *Zaznamenat* (viz kapitola 15.2).
2. Záznam *Http* je vhodný ke zpracování externími analytickými nástroji. Pro správce *Kerio Control* bude pravděpodobně přehlednější záznam *Web* (viz dále).

Příklad záznamu Http typu Apache

```
192.168.64.64 - rgabriel
[18/Apr/2011:15:07:17 +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/2011:15:07:17 +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 (*Kerio Control* ji 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“). V *Kerio Control* 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 (v *Kerio Control* vždy `DIRECT` = přímý přístup)
- `206.168.0.9` — IP adresa WWW serveru

24.11 Záznam Security

Informace, které souvisejí s bezpečností *Kerio Control* a lokální sítě. Záznam *Security* může obsahovat záznamy následujících kategorií:

1. *Záznamy systému prevence útoků*

   Záznamy o detekovaných útocích nebo o zachycené komunikaci z IP adres z internetových databází známých útočníků (tzv. černých listin) — podrobnosti viz kapitola 10.1.

Příklad

```
[02/Mar/2011 08:54:38] IPS: Packet drop, severity: High,
Rule ID: 1:2010575 ET TROJAN ASProtect/ASPack Packed Binary
proto:TCP, ip/port:95.211.98.71:80(hosted-by.example.com)
-> 192.168.48.131:49960(jnovak-pc.firma.cz,user:jnovak)
```

- `IPS: Packet drop` — pro daný typ útoku byla nastavena akce *Zaznamenat a zahodit* (v případě akce *Zaznamenat* se v záznamu zobrazí `IPS: Alert`)
- `severity: High` — úroveň závažnosti útoku
- `Rule ID: 1:2010575` — číselný identifikátor útoku (lze využít při definici výjimek v upřesňujícím nastavení systému detekce útoků)
- `ET TROJAN ASProtect/ASPack...` — název a popis útoku (u některých útoků není k dispozici)
- `proto:TCP` — použitý komunikační protokol
- `ip/port:95.211.98.71:80(hosted-by.example.com)` — zdrojová IP adresa a port v zachyceném paketu; v závorce DNS jméno příslušného počítače (pokud je zjistitelné)
- `-> 192.168.48.131:49960(jnovak-pc.firma.cz,user:jnovak)` — cílová IP adresa a port v zachyceném paketu; v závorce DNS jméno příslušného počítače (pokud je zjistitelné), případně jméno uživatele přihlášeného k firewallu z příslušné lokální stanice

2. *Záznamy funkce Anti-spoofing*

   Záznamy o paketech, které byly zachyceny funkcí *Anti-spoofing* (tzn. pakety s neplatnou zdrojovou IP adresou) — podrobnosti viz kapitola 10.3.

Příklad
```
[17/Jul/2011 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 7)
- `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

3. *Zprávy inspekčního modulu protokolu FTP*

Příklad 1
```
[17/Jul/2011 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/2011 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)

4. *Zprávy o neúspěšném ověření uživatelů*

Formát zprávy:

`Authentication: <služba>: Client: <IP adresa>: <důvod>`

- `<služba>` — služba *Kerio Control*, ke které se klient přihlašuje (`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 18.1 a 13.1.

5. *Informace o startu a ukončení Kerio Control Engine.*

   a) Start Engine:

   ```
   [17/Dec/2011 12:11:33] Engine: Startup.
   ```

   b) Ukončení Engine:

   ```
   [17/Dec/2011 12:22:43] Engine: Shutdown.
   ```

24.12 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/2011 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 v *Kerio Control* pro systém *Windows*.

24.13 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 *Kerio Control*, 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.

Kategorie varovných hlášení vypisovaných do záznamu *Warning*:

- Systémová varování (např. detekce známé konfliktní aplikace),
- Problémy s konfigurací *Kerio Control* (např. neplatné hodnoty načtené z konfiguračního souboru),
- Varovná hlášení při operacích prováděných *Kerio Control Engine* (např. DHCP, DNS, antivirová kontrola, ověřování uživatelů atd.),
- Varování týkající se licence (vypršení Software Maintenance nebo blížící se vypršení licence *Kerio Control*, modulu *Kerio Control Web Filter* nebo integrovaného antiviru),

  Poznámka:
  Vypršení licence (skončení funkčnosti produktu) je považováno za chybu — tato informace se zapisuje do záznamu *Error*.
- Varovná hlášení modulu *Řízení šířky pásma*,
- Varovná hlášení modulu *Kerio Control Web Filter*,
- Výpisy paměti po pádu aplikace.

Příklad záznamů v okně Warning

```
[15/Apr/2011 15:00:51] Authentication subsystem warning:
Kerberos 5 auth: user standa@firma.cz not authenticated
[15/Apr/2011 15:00:51] Authentication subsystem warning:
Invalid password for user admin
[16/Apr/2011 10:53:20] 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*.

24.14 Záznam Web

Tento záznam zobrazuje HTTP požadavky zpracované inspekčním modulem protokolu HTTP (viz kapitola 17.3) nebo vestavěným proxy serverem (viz kapitola 11.5). 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/2011 10:29:51] 192.168.44.128 standa
"Kerio Technologies" http://www.kerio.cz/
```

- `[24/Apr/2011 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 elementu `<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 25

Kerio VPN

Kerio Control 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*). *Kerio Control* obsahuje proprietární implementaci VPN (dále jen „*Kerio VPN*“).

Implementace VPN v *Kerio Control* 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 firewally *Kerio Control*, 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 v *Kerio Control* 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 *Kerio Control* dodávána aplikace *Kerio VPN Client* (podrobné informace viz samostatný manuál *Kerio VPN Client — Příručka uživatele*).

Poznámka:
Koncepce *Kerio VPN* předpokládá, že *Kerio Control* 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 v *Kerio Control* (resp. přímo doménové účty při použití *Active Directory* nebo *Open Directory* — viz kapitola 13.1).

- V *Kerio Control* lze sledovat statistické informace o VPN tunelech a VPN klientech, podobně jako v případě fyzických rozhraní (podrobnosti viz kapitola 22.2).

25.1 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 25.2 a 25.3.

VPN server se zobrazuje jako speciální rozhraní v sekci *Konfigurace* → *Rozhraní*, záložka *Rozhraní*.

VPN subsíť a SSL certifikát

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) *Kerio Control* 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!
> *Kerio Control* 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.
> 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 18.1.

SSL certifikát

Informace o aktuálním certifikátu VPN serveru. Tento certifikát slouží k ověření identity serveru při vytváření VPN tunelu (podrobnosti viz kapitola 25.3). VPN server v *Kerio Control* 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 25.3).

> ***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 aplikace *Kerio Control* pod názvem `vpn.crt` a příslušný privátní klíč pod názvem `vpn.key`.
Postupy vytvoření a importu SSL certifikátu jsou podrobně popsány v kapitole 14.1.

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 v *Kerio Control* nabízí tyto možnosti konfigurace DNS serverů:

- *DNS server v Kerio Control* — VPN klientům bude jako primární DNS server nastavena IP adresa příslušného rozhraní počítače s *Kerio Control* — VPN klienti budou používat modul *DNS* (viz kapitola 11.1). Toto je výchozí volba, pokud je modul *DNS* v *Kerio Control* 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* v *Kerio Control*.

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 18.1).

- DNS doménu je potřeba specifikovat, pokud se jedná o doménu *Open Directory*, doménu *Windows NT* nebo síť bez domény, případně v situaci, kdy chceme VPN klientům nastavit jinou příponu domény (např. při mapování více domén).

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*).

Kerio Control 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 *Kerio Control* 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 24.8) 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.
   ```

   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 25.4).

> ***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.

25.2 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 v *Kerio Control* (viz kapitola 18.1).
- Připojení k VPN serveru z Internetu a komunikace mezi VPN klienty musí být povoleny komunikačními pravidly.

> ***Tip:***
> Přehled VPN klientů aktuálně připojených k firewallu lze zobrazit v administračním rozhraní v sekci *Stav → VPN klienti*. Podrobnosti viz kapitola 21.4.

Základní nastavení komunikačních pravidel pro VPN klienty

Jméno	Zdroj	Cíl	Služba	Akce
Kerio VPN Server	Libovolný	Firewall	Kerio VPN	Povolit
Lokální komunikace	Firewall Důvěryhodná / lokální rozhraní VPN klienti Všechny VPN tunely	Firewall Důvěryhodná / lokální rozhraní VPN klienti Všechny VPN tunely	Libovolný	Povolit

Obrázek 25.1 Obecná komunikační pravidla pro VPN klienty

- První pravidlo povoluje připojení k VPN serveru v *Kerio Control* 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 25.5.

Poznámka:

1. Při vytváření komunikačních pravidel pomocí *Průvodce komunikačními pravidly* mohou být výše popsaná pravidla vytvořena automaticky. V průvodci stačí zaškrtnout volbu *Kerio VPN server* (povolení připojení k VPN serveru z Internetu). Podrobnosti viz kapitola 9.1.
2. Pro přístup do Internetu používá každý VPN klient své stávající internetové připojení. VPN klienti nemohou přistupovat přes *Kerio Control* do Internetu (klientům nelze změnit nastavení výchozí brány).
3. Podrobné informace o definici komunikačních pravidel naleznete v kapitole 9.

25.3 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 *Kerio Control* včetně podpory VPN (v typické instalaci je podpora VPN obsažena).

Poznámka:
Každá instalace *Kerio Control* vyžaduje samostatnou licenci (viz kapitola 5).

Nastavení VPN serverů

Nejprve je třeba na obou stranách (koncích tunelu) povolit a nastavit VPN server. Podrobnosti o konfiguraci VPN serveru naleznete v kapitole 25.1.

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.

Jméno tunelu
: Každému VPN tunelu musí být přiřazeno jednoznačné jméno. Pod tímto jménem se tunel zobrazuje v tabulce rozhraní, v komunikačních pravidlech (viz kapitola 9.3) a ve statistikách rozhraní (viz kapitola 22.2).

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 `85.17.210.230:9000`).
    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.

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* v *Kerio Control*, můžeme v pravidlech pro předávání DNS dotazů (viz kapitola 11.1) 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.

Postup konfigurace DNS je podrobně popsán na příkladu v kapitole 25.5.

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 25.4.

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 pravidelných časových intervalech), 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 25.2), pak jsou tyto podmínky splněny.

Jméno	Zdroj	Cíl	Služba	Akce
Kerio VPN Server	Libovolný	Firewall	Kerio VPN	Povolit
Lokální komunikace	Firewall Důvěryhodná / lokální rozhraní VPN klienti Všechny VPN tunely	Firewall Důvěryhodná / lokální rozhraní VPN klienti Všechny VPN tunely	Libovolný	Povolit

Obrázek 25.2 Komunikační pravidla pro VPN tunel

Poznámka:
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 25.5.

25.4 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 v *Kerio Control*.

Pro ošetření uvedených situací lze v dialogu pro definici VPN tunelu (viz kapitola 25.3), resp. pro nastavení VPN serveru (viz kapitola 25.1) 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 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).

25.5 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 25.6.

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 Control — Konfigurace krok za krokem*.

Zadání

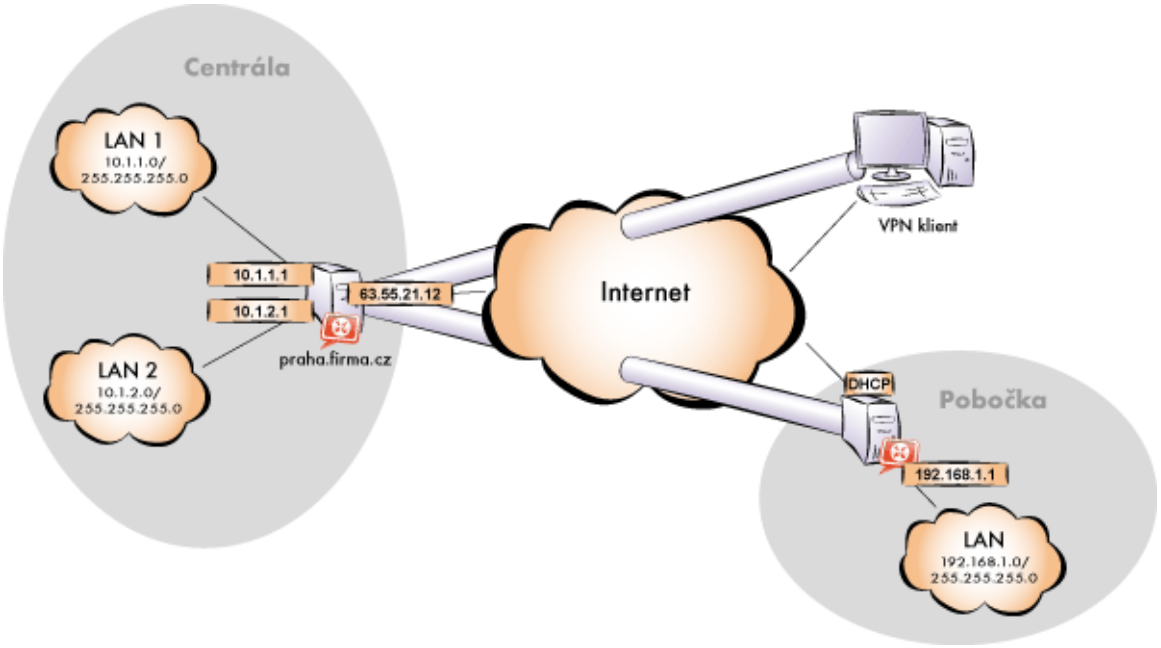
Fiktivní firma má centrálu v Praze a pobočku v Plzni. Lokální sítě centrály a pobočky mají být propojeny VPN tunelem za použití *Kerio VPN*. Do sítě centrály má být umožněn přístup VPN klientům.

Server (výchozí brána) centrály má pevnou veřejnou IP adresu `85.17.210.230` (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 25.3.



Obrázek 25.3 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 *Kerio Control*.

   Pro *každou* instalaci *Kerio Control* je potřeba samostatná licence pro příslušný počet uživatelů! Podrobnosti viz kapitola 5.

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 *Kerio Control*.

Jedná-li se o novou (čistou) instalaci *Kerio Control*, můžeme využít průvodce připojením (viz kapitola 8.1) a průvodce komunikačními pravidly (viz kapitola 9.1).

Podrobný popis základní konfigurace *Kerio Control* a lokální sítě je uveden v samostatném manuálu *Kerio Control — 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 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 tabulky jmen počítačů (v případě statických IP adres) nebo nastavením spolupráce modulu *DNS* s DHCP serverem (v případě dynamicky přidělovaných IP adres). Podrobnosti viz kapitola 11.1.

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` (`traceroute`). 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 *Kerio Control*.

2. Provedeme základní konfiguraci *Kerio Control* pomocí průvodce připojením (viz kapitola 8.1) a průvodce komunikačními pravidly (viz kapitola 9.1).

   V průvodci komunikačními pravidly povolíme přístup ke službě *Kerio VPN server*. 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
Kerio VPN Server	Libovolný	Firewall	Kerio VPN	Povolit
Lokální komunikace	Firewall Důvěryhodná / lokální rozhraní VPN klienti Všechny VPN tunely	Firewall Důvěryhodná / lokální rozhraní VPN klienti Všechny VPN tunely	Libovolný	Povolit

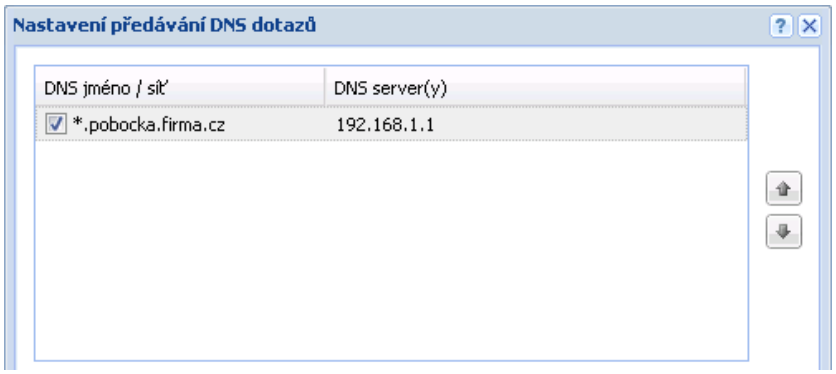
Obrázek 25.4 Centrála — výchozí komunikační pravidla pro Kerio VPN

   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* v *Kerio Control* 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 *Kerio Control* na protější straně tunelu (tj. rozhraní připojeného do lokální sítě na protější straně).



Obrázek 25.5 Centrála — nastavení předávání DNS dotazů

- Na rozhraních počítače s *Kerio Control* připojených do lokálních sítí *LAN 1* a *LAN 2* nebude nastaven žádný DNS server.
- Na ostatních počítačích nastavíme jako upřednostňovaný (primární) DNS server IP adresu shodnou s příslušnou výchozí bránou (`10.1.1.1`, resp. `10.1.2.1`). Počítače v lokální síti samozřejmě mohou být konfigurovány automaticky protokolem DHCP.

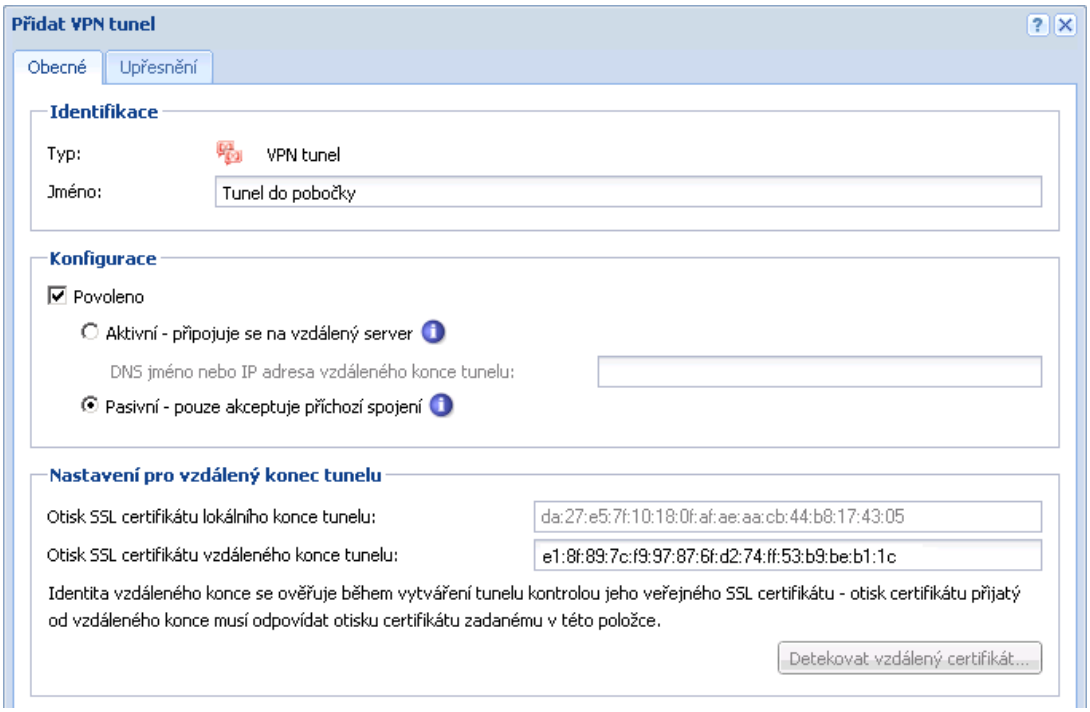
Poznámka:
Pro správnou funkci DNS musí DNS databáze obsahovat záznamy o počítačích v příslušné lokální síti. Toho lze docílit zapsáním IP adres a DNS jmen lokálních počítačů do tabulky jmen počítačů (v případě statických IP adres) nebo nastavením spolupráce modulu *DNS* s DHCP serverem (v případě dynamicky přidělovaných IP adres). Podrobnosti viz kapitola 11.1.

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.

   Podrobnosti o konfiguraci VPN serveru viz kapitola 25.1.

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 25.6 Centrála — definice VPN tunelu do pobočky

6. Upravíme komunikační pravidla dle požadavků na omezení přístupu.

Jméno	Zdroj	Cíl	Služba	Akce
Kerio VPN Server	Libovolný	Firewall	Kerio VPN	Povolit
Lokální komunikace	Firewall Důvěryhodná / lokální	Firewall Důvěryhodná / lokální	Libovolný	Povolit
VPN klienti	VPN klienti	LAN 1 Tunel do pobočky	Libovolný	Povolit
Pobočka	Tunel do pobočky	LAN 1	Libovolný	Povolit
Centrála	Důvěryhodná / lokální	Tunel do pobočky	Libovolný	Povolit

Obrázek 25.7 Centrála — výsledná komunikační pravidla

- V pravidle *Lokální komunikace* ponecháme pouze lokální síť centrály firmy, tj. firewall a skupinu *Důvěryhodná / Lokální rozhraní*.
- 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 lokální sítě centrály do sítě pobočky.

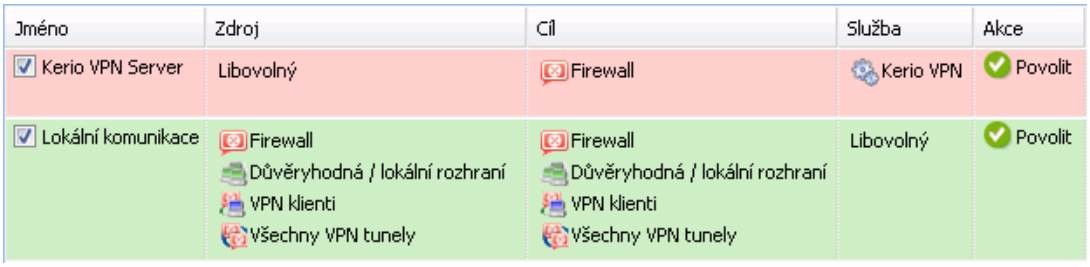
Takto definovaná pravidla splňují všechny požadavky na povolení a omezení přístupu mezi centrálou, pobočkou a VPN klienty. Komunikace, která nevyhoví těmto pravidlům, bude implicitně blokována výchozím pravidlem (viz kapitola 9.3).

Konfigurace v pobočce firmy

1. Na výchozí bránu sítě pobočky (dále jen „server“) nainstalujeme *Kerio Control*.
2. Provedeme základní konfiguraci *Kerio Control* pomocí průvodce připojením (viz kapitola 8.1) a průvodce komunikačními pravidly (viz kapitola 9.1).

   Povolovat službu *Kerio VPN server* v tomto případě nemá smysl (server má dynamickou veřejnou IP adresu).

   Tím dojde k vytvoření pravidel pro připojení k VPN serveru a pro komunikaci VPN klientů s lokální sítí, resp. firewallem.



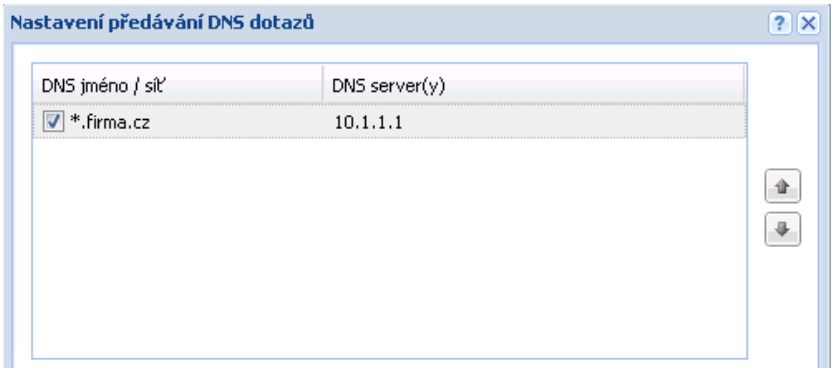
Obrázek 25.8 Pobočka — výchozí komunikační pravidla pro Kerio VPN

Po vytvoření VPN tunelu tato pravidla upravíme (viz 6. krok).

3. Nastavíme DNS (resp. upravíme nastavení DNS):

   - V konfiguraci modulu *DNS* v *Kerio Control* 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 *Kerio Control* na protější straně tunelu (tj. rozhraní připojeného do lokální sítě na protější straně).



Obrázek 25.9 Pobočka — nastavení předávání DNS dotazů

   - Na rozhraní počítače s *Kerio Control* připojeném do lokální sítě nebude nastaven žádný DNS server.

   - Na ostatních počítačích nastavíme jako upřednostňovaný (primární) DNS server IP adresu shodnou s příslušnou výchozí bránou (`192.168.1.1`). Počítače v lokální síti samozřejmě mohou být konfigurovány automaticky protokolem DHCP.

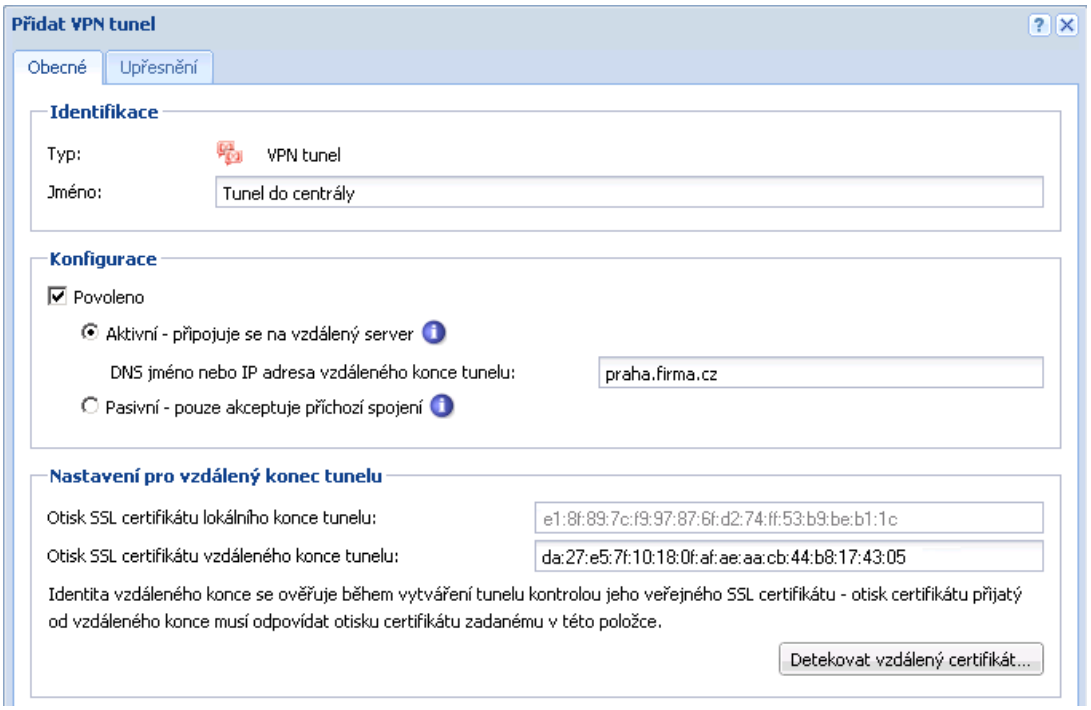
Poznámka:
Pro správnou funkci DNS musí DNS databáze obsahovat záznamy o počítačích v příslušné lokální síti. Toho lze docílit zapsáním IP adres a DNS jmen lokálních počítačů do tabulky jmen počítačů (v případě statických IP adres) nebo nastavením spolupráce modulu *DNS* s DHCP serverem (v případě dynamicky přidělovaných IP adres). Podrobnosti viz kapitola 11.1.

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.

   Podrobnosti o konfiguraci VPN serveru viz kapitola 25.1.

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.



Obrázek 25.10 Pobočka — definice VPN tunelu do centrály

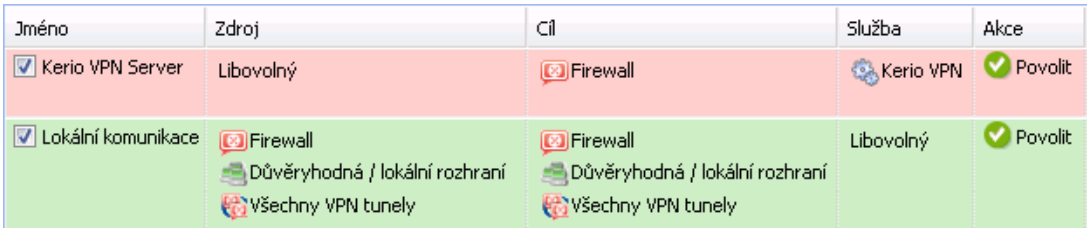
   V tomto okamžiku by mělo dojít ke spojení — navázání tunelu. Je-li spojení úspěšné, zobrazí se u obou konců tunelu ve sloupci *Informace o adaptéru* stav *Připojeno*. Nedojde-li k navázání spojení, doporučujeme prověřit nastavení komunikačních pravidel a dostupnost vzdáleného serveru — v našem příkladu 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 25.3.

6. Z komunikačního pravidla *Lokální komunikace* můžeme odstranit skupinu *Všichni VPN klienti* (do pobočky se žádní VPN klienti připojovat nemohou).



Obrázek 25.11 Pobočka — výsledná komunikační pravidla

Poznámka:
Žádné další úpravy komunikačních pravidel není třeba provádět. Požadovaná omezení přístupu jsou již zajištěna komunikačními pravidly na serveru centrály.

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` (`traceroute`). 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.

25.6 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).

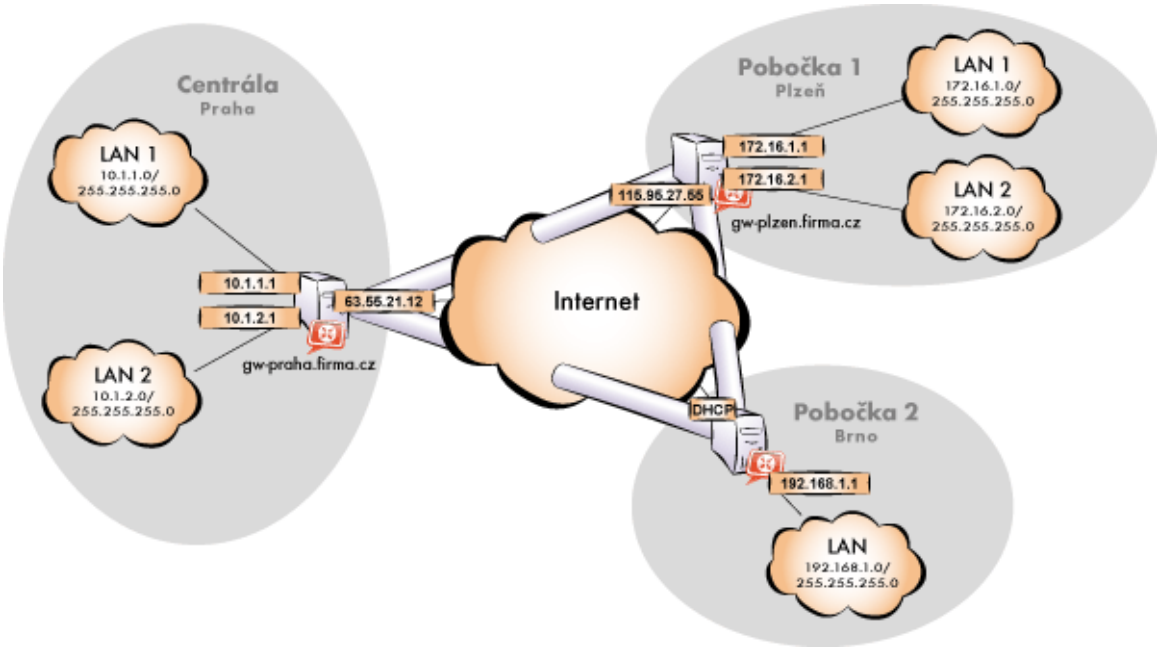
Oproti VPN bez redundantních cest (viz kapitola 25.5) se konfigurace *Kerio VPN* liší pouze v nastavení směrování mezi konci jednotlivých tunelů. V tomto případě je třeba nastavit směrování mezi jednotlivými konci VPN tunelů ručně, použití automatické výměny cest není vhodné. Důvodem je, že *Kerio VPN* nepoužívá žádný směrovací protokol a výměna cest probíhá pouze na základě porovnání směrovacích tabulek na jednotlivých koncích VPN tunelu (viz též kapitola 25.4). 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 25.5.

Zadání

Předpokládejme schéma sítě dle obrázku 25.12.



Obrázek 25.12 Příklad konfigurace VPN — firma se dvěma pobočkami

Server (výchozí brána) centrály má pevnou veřejnou IP adresu `85.17.210.230` (DNS jméno `gw-praha.firma.cz`). Server první pobočky má IP adresu `195.39.22.12` (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.

Obecný postup

Ve všech lokálních sítích (tj. v centrále i v obou pobočkách firmy) je třeba provést tyto kroky:

1. Na výchozí bránu sítě nainstalujeme aplikaci *Kerio Control*.

Poznámka:
Pro *každou* instalaci *Kerio Control* je potřeba samostatná licence pro příslušný počet uživatelů! Podrobnosti viz kapitola 5.

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 *Kerio Control*.

   Jedná-li se o novou (čistou) instalaci *Kerio Control*, můžeme využít průvodce připojením (viz kapitola 8.1) a průvodce komunikačními pravidly (viz kapitola 9.1).

   Podrobný popis základní konfigurace *Kerio Control* a lokální sítě je uveden v samostatném manuálu *Kerio Control — 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 správnou funkci DNS musí být specifikován alespoň jeden DNS server, na který budou předávány DNS dotazy do ostatních domén (typicky DNS server poskytovatele internetového připojení).

   Poznámka:
   DNS databáze musí obsahovat záznamy o počítačích v příslušné lokální síti. Toho lze docílit zapsáním IP adres a DNS jmen lokálních počítačů do tabulky jmen počítačů (v případě statických IP adres) a/nebo nastavením spolupráce *DNS* s DHCP serverem (v případě dynamicky přidělovaných IP adres). Podrobnosti viz kapitola 11.1.

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 25.5.

8. Z každé lokální sítě otestujeme dostupnost počítačů v obou vzdálených sítích. Pro tento test můžeme použít systémové příkazy `ping` a `tracert` (`traceroute`). 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 aplikaci *Kerio Control*.

2. V *Kerio Control* nastavíme základní komunikační pravidla pomocí průvodce připojením (viz kapitola 8.1) a průvodce komunikačními pravidly (viz kapitola 9.1).

   V průvodci komunikačními pravidly povolíme přístup ke službě *Kerio VPN server*.

   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
Kerio VPN Server	Libovolný	Firewall	Kerio VPN	Povolit
Lokální komunikace	Firewall Důvěryhodná / lokální rozhraní VPN klienti Všechny VPN tunely	Firewall Důvěryhodná / lokální rozhraní VPN klienti Všechny VPN tunely	Libovolný	Povolit

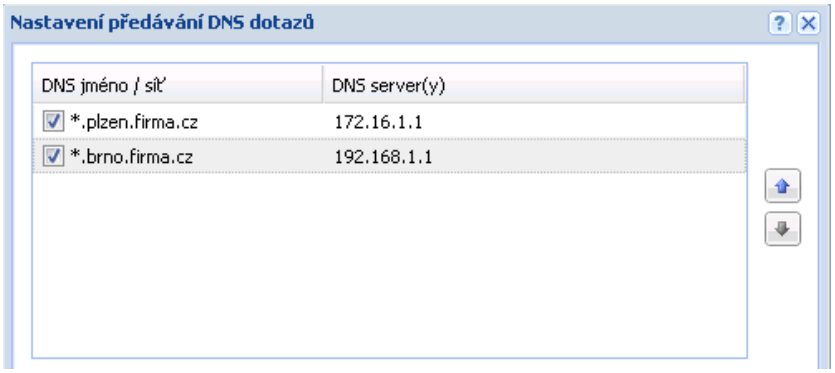
Obrázek 25.13 Centrála — výchozí komunikační pravidla pro Kerio VPN

3. Nastavíme DNS (resp. upravíme nastavení DNS):

   - V konfiguraci modulu *DNS* v *Kerio Control* 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 *Kerio Control* na protější straně příslušného tunelu (tj. rozhraní připojeného do lokální sítě na protější straně tunelu).



Obrázek 25.14 Centrála — nastavení předávání DNS dotazů

- Na rozhraních počítače s *Kerio Control* připojených do lokálních sítí *LAN 1* a *LAN 2* nebude nastaven žádný DNS server.
- Na ostatních počítačích nastavíme jako upřednostňovaný (primární) DNS server IP adresu shodnou s příslušnou výchozí bránou (`10.1.1.1`, resp. `10.1.2.1`). Počítače v lokální síti samozřejmě mohou být konfigurovány automaticky protokolem DHCP.

4. Povolíme VPN server, případně nastavíme jeho SSL certifikát (nemáme-li certifikát vystavený důvěryhodnou certifikační autoritou, vytvoříme certifikát podepsaný sám sebou).

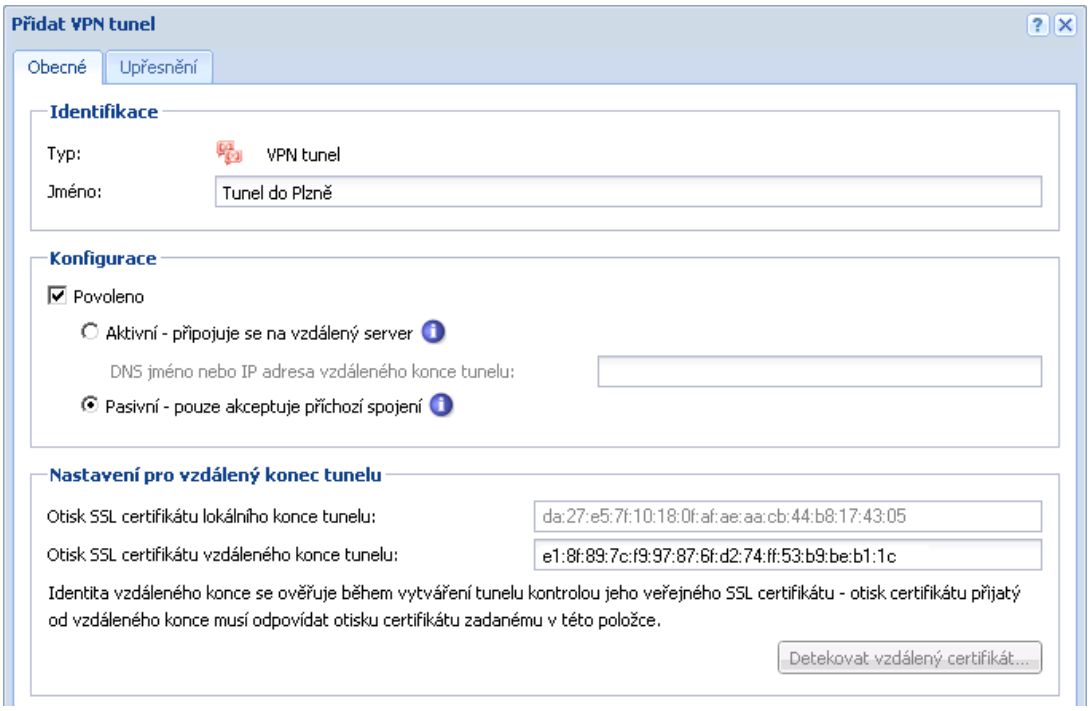
   Poznámka:
   V položkách *VPN subsíť* a *Maska* je nyní uvedena automaticky vybraná volná subsíť. Zkontrolujeme, zda tato subsíť nekoliduje s žádnou subsítí v centrále a na pobočkách, případně zadáme jinou (volnou) subsíť.

   Podrobnosti o konfiguraci VPN serveru viz kapitola 25.1.

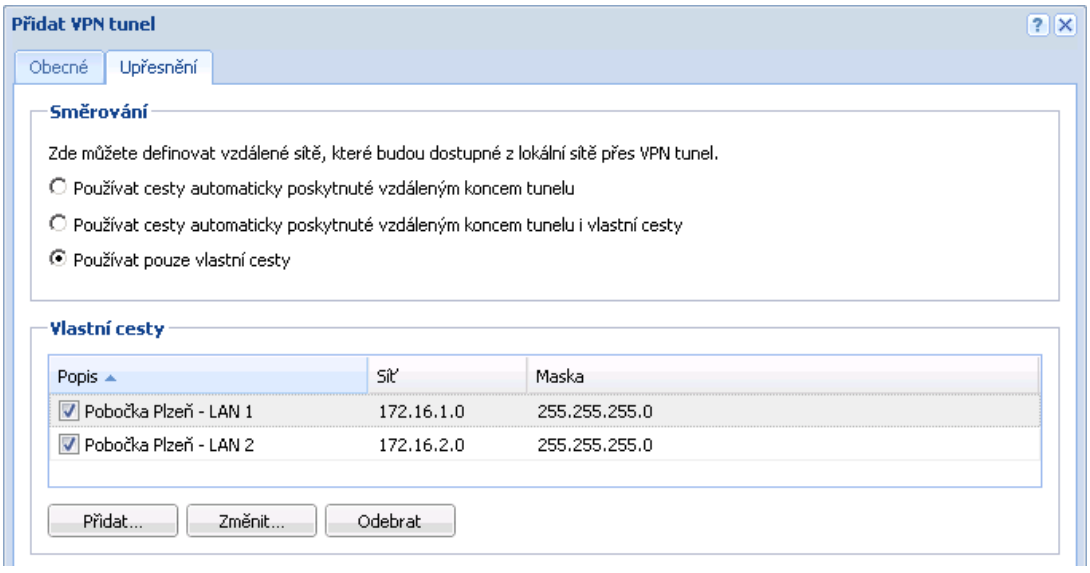
5. Vytvoříme pasivní konec VPN tunelu do pobočky *Plzeň*. Jako otisk vzdáleného SSL certifikátu zadáme otisk certifikátu VPN serveru na v pobočce *Plzeň*.

   V záložce *Upřesnění* zvolíme *Používat pouze vlastní cesty* a nastavíme cesty do subsítí na

vzdáleném konci tunelu (tj. v pobočce *Plzeň*).



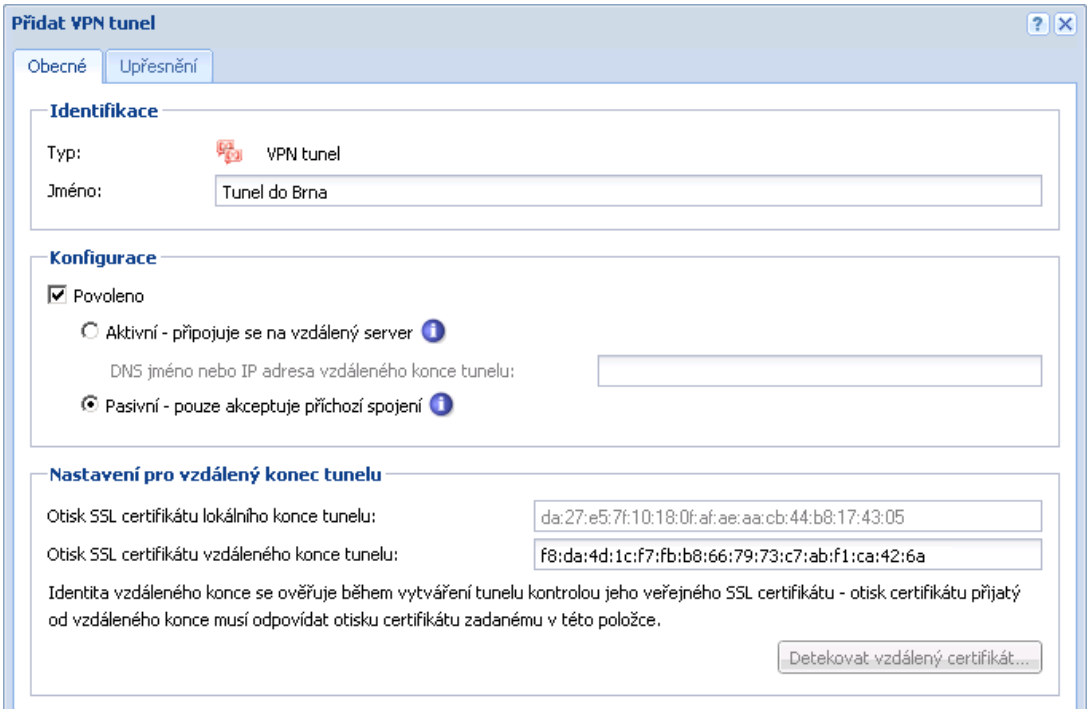
Obrázek 25.15 Centrála — definice VPN tunelu do pobočky Plzeň



Obrázek 25.16 Centrála — nastavení směrování pro tunel do pobočky Plzeň

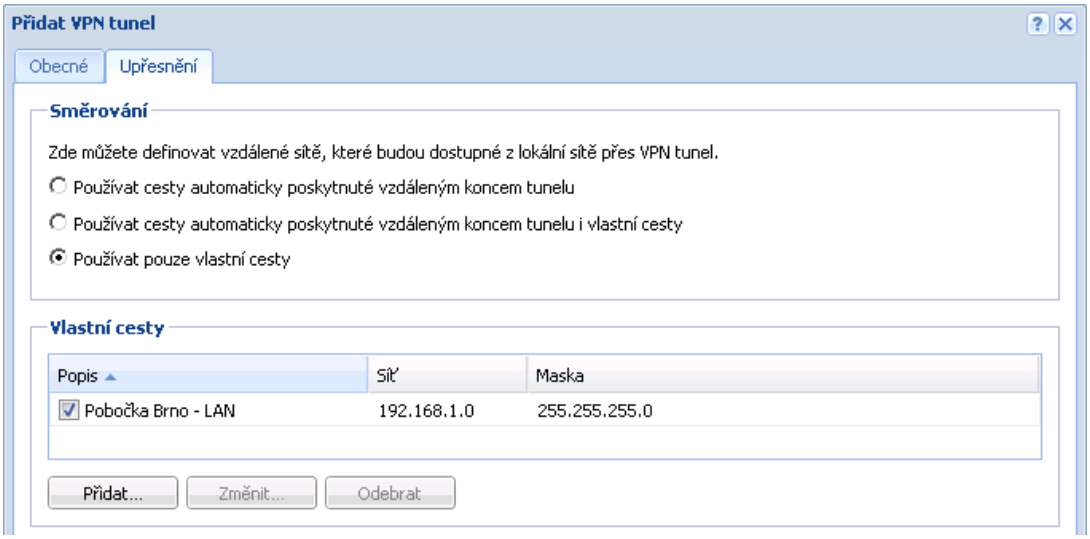
> ***Upozornění:***
> V případě konfigurace VPN podle uvažovaného schématu (viz obrázek 25.12) *nedoporučujeme* používat automaticky poskytnuté cesty! Při automatické výměně cest nebude směrování v rámci VPN optimální (např. veškerá komunikace mezi *centrálou* a pobočkou *Brno* bude směrována přes pobočku *Plzeň*, přičemž tunel mezi *centrálou* a pobočkou *Brno* zůstane nevyužitý).

6. Obdobným způsobem vytvoříme pasivní konec tunelu do pobočky *Brno*.



Obrázek 25.17 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*).



Obrázek 25.18 Centrála — nastavení směrování pro tunel do pobočky Brno

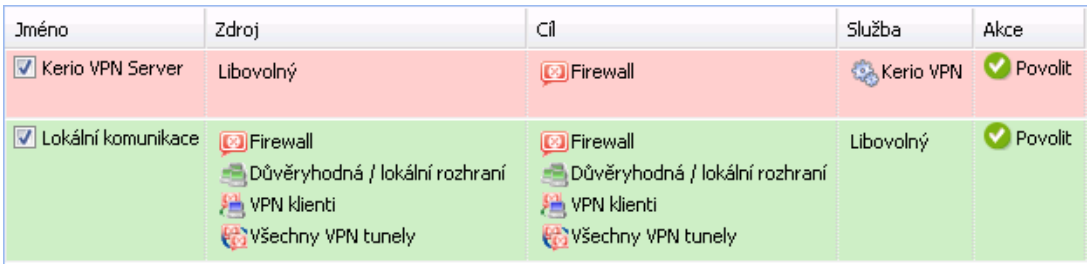
Konfigurace v pobočce Plzeň

1. Na výchozí bránu sítě pobočky nainstalujeme *Kerio Control*.

2. V *Kerio Control* nastavíme základní komunikační pravidla pomocí průvodce připojením (viz kapitola 8.1) a průvodce komunikačními pravidly (viz kapitola 9.1).

   V průvodci komunikačními pravidly povolíme přístup ke službě *Kerio VPN server*.

   Tím dojde k vytvoření pravidel pro připojení k VPN serveru a pro komunikaci VPN klientů s lokální sítí, resp. firewallem.

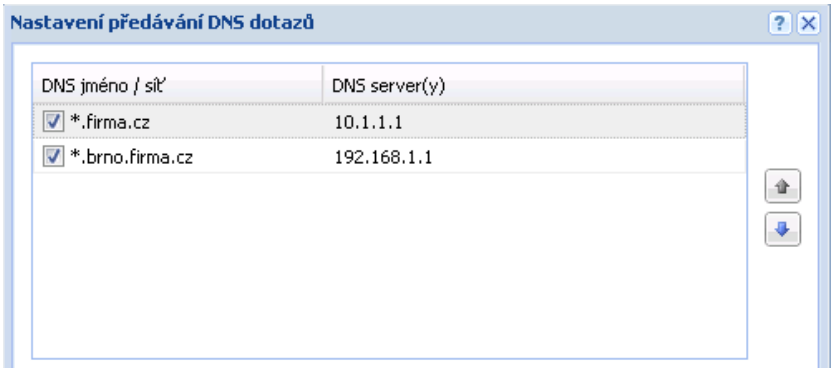


Obrázek 25.19 Pobočka Plzeň — výchozí komunikační pravidla pro Kerio VPN

3. Nastavíme DNS (resp. upravíme nastavení DNS):

   - V konfiguraci modulu *DNS* v *Kerio Control* 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 *Kerio Control* na protější straně příslušného tunelu (tj. rozhraní připojeného do lokální sítě na protější straně).



Obrázek 25.20 Pobočka Plzeň — nastavení předávání DNS dotazů

- Na rozhraních počítače s *Kerio Control* připojených do lokálních sítí *LAN 1* a *LAN 2* nebude nastaven žádný DNS server.

- Na ostatních počítačích nastavíme jako upřednostňovaný (primární) DNS server IP adresu shodnou s příslušnou výchozí bránou (`172.16.1.1`, resp. `172.16.2.1`). Počítače v lokální síti samozřejmě mohou být konfigurovány automaticky protokolem DHCP.

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.

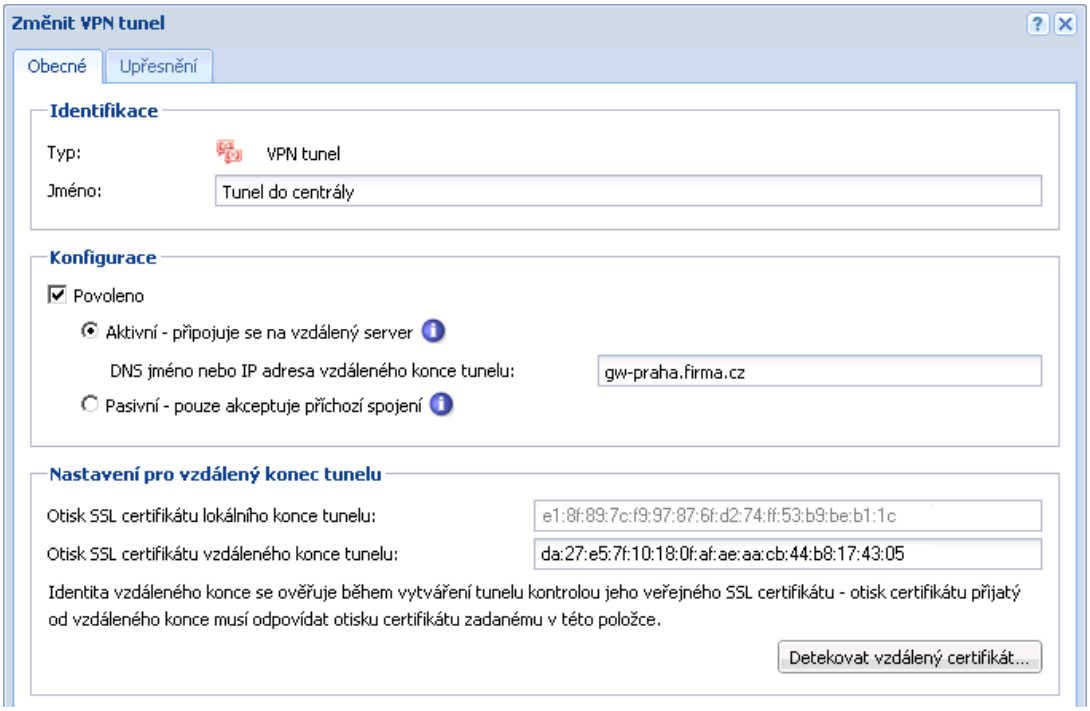
   Podrobnosti o konfiguraci VPN serveru viz kapitola 25.1.

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.

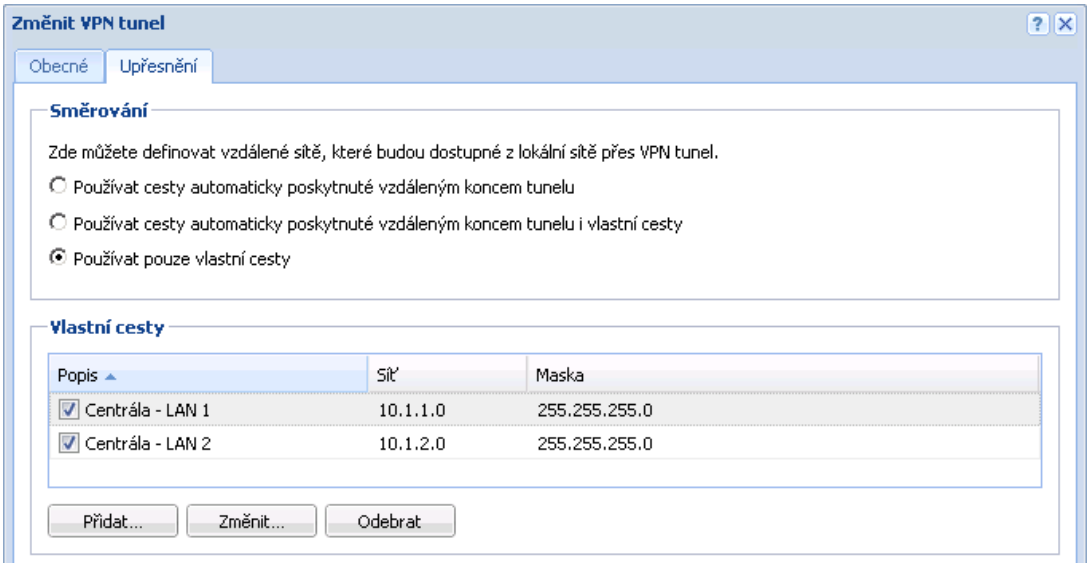
   V záložce *Upřesnění* zvolíme *Používat pouze vlastní cesty* a nastavíme cesty do lokálních sítí v *centrále*.

   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
   ```



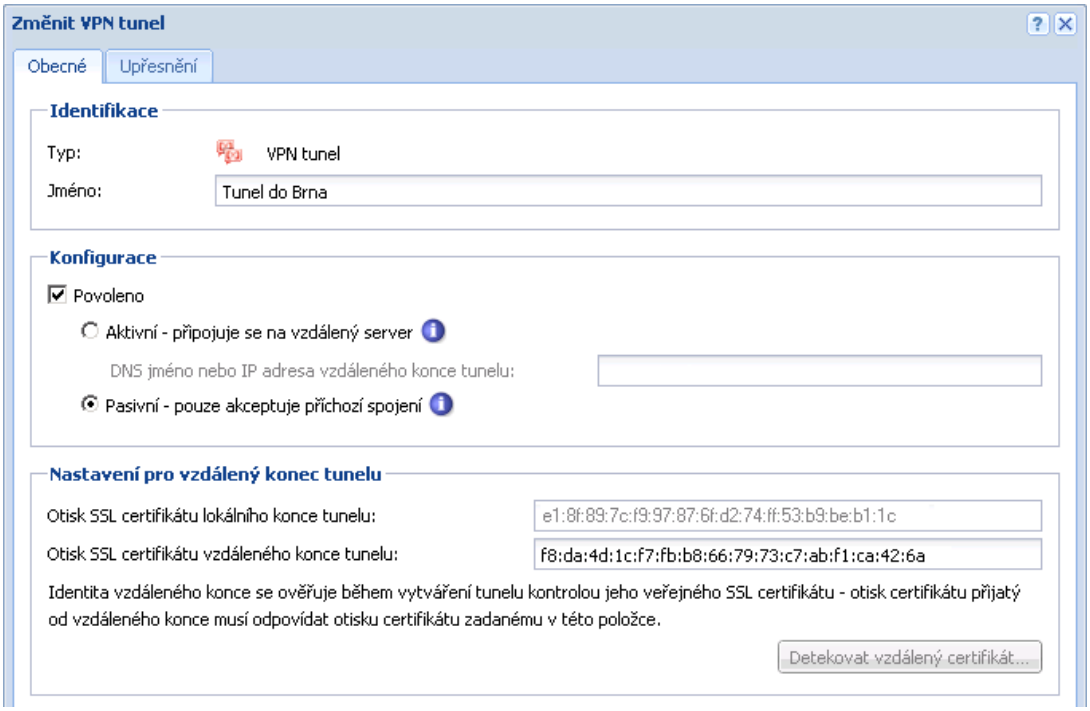
Obrázek 25.21 Pobočka Plzeň — definice VPN tunelu do centrály



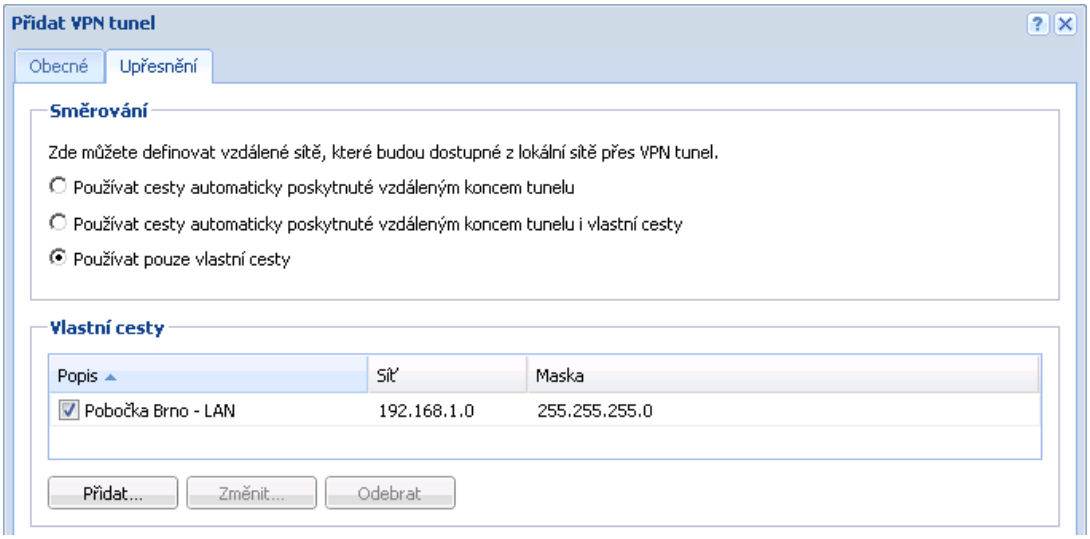
Obrázek 25.22 Pobočka Plzeň — nastavení směrování pro tunel do centrály

6. Vytvoříme pasivní konec tunelu do pobočky *Brno*. Jako otisk vzdáleného SSL certifikátu zadáme otisk certifikátu VPN serveru v pobočce *Brno*.

   V záložce *Upřesnění* zvolíme *Používat pouze vlastní cesty* a nastavíme cesty do lokálních sítí v pobočce *Brno*.



Obrázek 25.23 Pobočka Plzeň — definice VPN tunelu do pobočky Brno



Obrázek 25.24 Pobočka Plzeň — nastavení směrování pro tunel do pobočky Brno

Konfigurace v pobočce Brno

1. Na výchozí bránu sítě pobočky nainstalujeme *Kerio Control*.

2. V *Kerio Control* nastavíme základní komunikační pravidla pomocí průvodce připojením (viz kapitola 8.1) a průvodce komunikačními pravidly (viz kapitola 9.1).

   Povolovat službu *Kerio VPN server* v tomto případě nemá smysl (server má dynamickou veřejnou IP adresu).

3. Nastavíme DNS (resp. upravíme nastavení DNS):

   - V konfiguraci modulu *DNS* v *Kerio Control* 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 *Kerio Control* na protější straně tunelu (tj. rozhraní připojeného do lokální sítě na protější straně).

Obrázek 25.25 Pobočka Brno — nastavení předávání DNS dotazů

   - Na rozhraní počítače s *Kerio Control* připojeném do lokální sítě *LAN* nebude nastaven žádný DNS server.

   - Na ostatních počítačích rovněž nastavíme jako upřednostňovaný (primární) DNS server IP adresu `192.168.1.1`.

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 25.1.

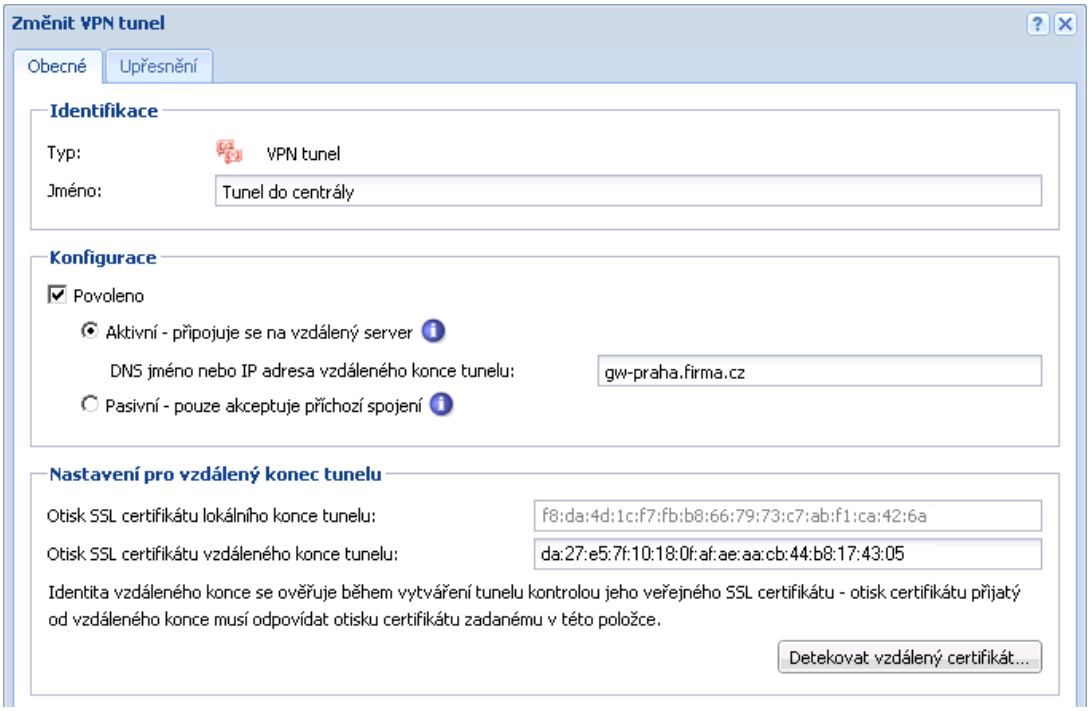
5. Vytvoříme aktivní konec VPN tunelu připojující se k serveru centrály (`praha.firma.cz`). Jako otisk vzdáleného SSL certifikátu zadáme otisk certifikátu VPN serveru v centrále.

   V záložce *Upřesnění* zvolíme *Používat pouze vlastní cesty* a nastavíme cesty do lokálních sítí v *centrále*.

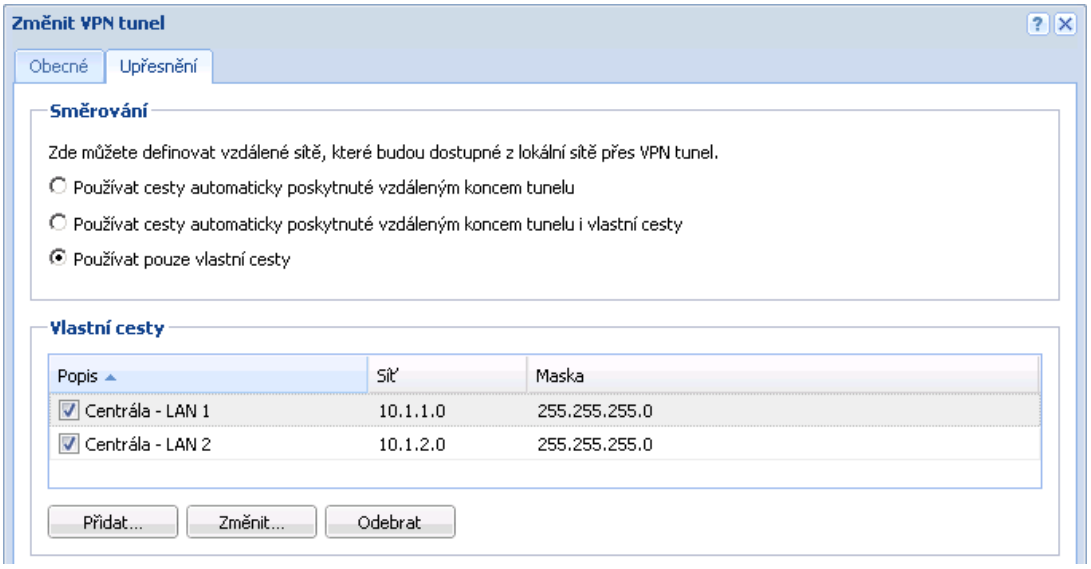
   V tomto okamžiku by mělo dojít ke spojení — navázání tunelu. Je-li spojení úspěšné, zobrazí se u obou konců tunelu ve sloupci *Informace o adaptéru* stav *Připojeno*. Nedojde-li k navázání spojení, doporučujeme prověřit nastavení komunikačních pravidel

a dostupnost vzdáleného serveru — v našem příkladu můžeme na serveru pobočky *Brno* zadat příkaz

```
ping gw-praha.firma.cz
```

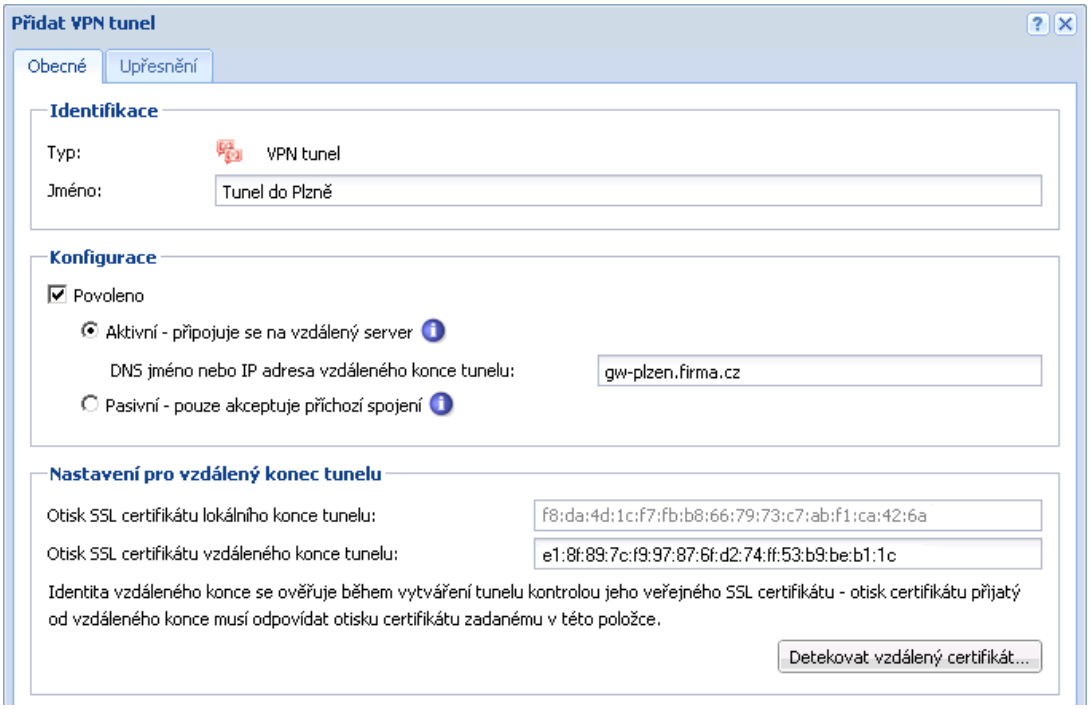


Obrázek 25.26 Pobočka Brno — definice VPN tunelu do centrály



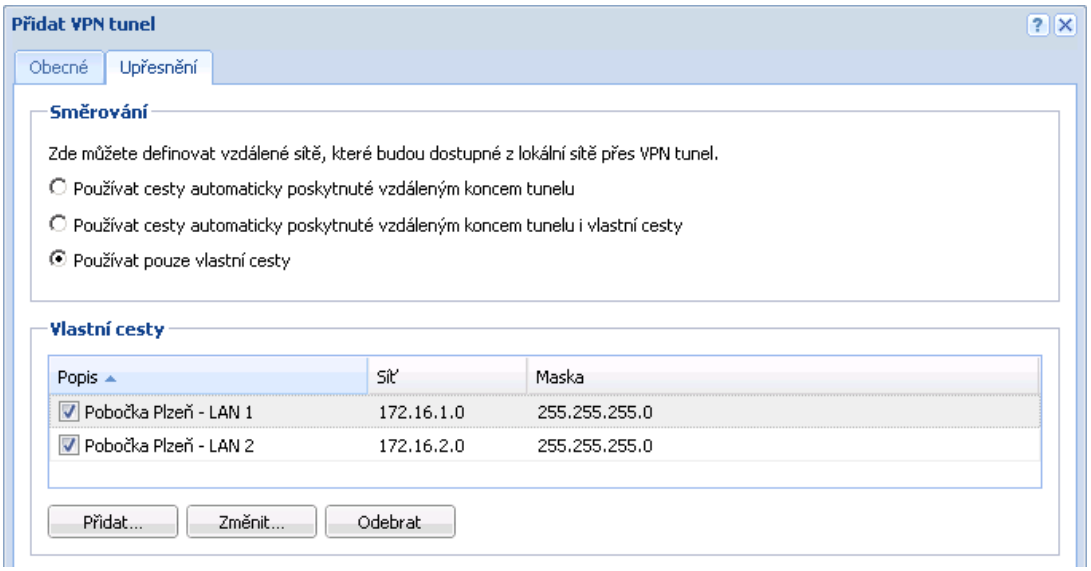
Obrázek 25.27 Pobočka Brno — nastavení směrování pro tunel do centrály

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 25.28 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*.



Obrázek 25.29 Pobočka Brno — nastavení směrování pro tunel do pobočky 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. Z komunikačního pravidla *Lokální komunikace* můžeme odstranit skupinu *Všichni VPN klienti* (do této pobočky se žádní VPN klienti připojovat nemohou).

Jméno	Zdroj	Cíl	Služba	Akce
Kerio VPN Server	Libovolný	Firewall	Kerio VPN	Povolit
Lokální komunikace	Firewall Důvěryhodná / lokální rozhraní Všechny VPN tunely	Firewall Důvěryhodná / lokální rozhraní Všechny VPN tunely	Libovolný	Povolit

Obrázek 25.30 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` (`traceroute`).

Kapitola 26

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 *Kerio Control* chrání. Toto rozhraní je k dispozici pouze v *Kerio Control* na operačním systému *Windows*.

Rozhraní *SSL-VPN* je do jisté míry alternativou k aplikaci *Kerio VPN Client* (viz kapitola 25). 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 Control — Příručka uživatele*.

26.1 Konfigurace SSL-VPN v Kerio Control

Podmínky pro správnou funkci rozhraní SSL-VPN

Pro správnou funkci rozhraní *SSL-VPN* musejí být splněny tyto podmínky:

1. Počítač s *Kerio Control* 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 v *Kerio Control* uděleno právo používat *Clientless SSL-VPN* (viz kapitola 18.2).

4. Je-li *Kerio Control* 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 nastavit v sekci *Konfigurace* → *Další volby*, záložka *SSL-VPN*.

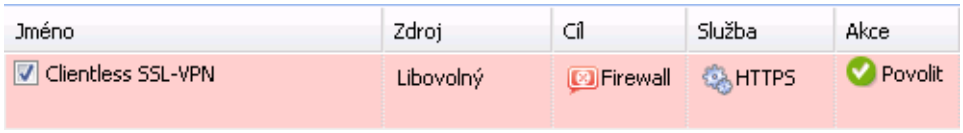
Výchozím portem pro rozhraní *SSL-VPN* je port `443` (jedná se o standardní port služby *HTTPS*).

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 *Kerio Control* nebo VPN serveru a je podrobně popsán v kapitole 14.1.

> ***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. Toto pravidlo může být vytvořeno automaticky zaškrtnutím volby *Clientless SSL-VPN* v *Průvodci komunikačními pravidly* (viz kapitola 9.1), případně jej můžeme kdykoliv později vytvořit ručně (viz kapitola 9.4).



Obrázek 26.1 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 v *Kerio Control* aktivní antivirový modul (viz kapitola 16), 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 16.5.

26.2 Použití rozhraní SSL-VPN

Pro přístup k rozhraní lze využít většinu běžných grafických WWW prohlížečů (viz kapitola 2.2). Do prohlížeče zadáme URL ve tvaru

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

kde `server` je DNS jméno nebo IP adresa počítače s *Kerio Control*. 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 27

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 *Kerio Control* ve vaší síti.

27.1 Vytvoření USB flash disku pro instalaci Software Appliance

Kerio Control v edici Appliance je distribuována ve formě ISO obrazu instalačního CD. Tento ISO obraz lze využít také k vytvoření bootovatelného USB flash disku.

Vyberte si postup podle vaší platformy:

Microsoft Windows

1. Připojte USB flash disk k vašemu počítači. V případě potřeby zálohujte soubory, které jsou na něm uložené. Obsah flash disku bude kompletně přepsán!
2. Stáhněte si a rozbalte program Image Writer (program není potřeba instalovat).
3. V programu *Image Writer* nalistujte soubor s ISO obrazem, vyberte písmeno vašeho USB flash disku a stiskněte tlačítko *Write*.
4. Bezpečně odeberte zařízení a odpojte USB flash disk od vašeho počítače.

Linux

1. Připojte USB flash disk k vašemu počítači. V případě potřeby zálohujte soubory, které jsou na něm uložené. Obsah flash disku bude kompletně přepsán!
2. Spusťte terminál (konzoli) s právy superuživatele (např. příkazy `su` nebo `sudo -s` — dle vaší linuxové distribuce).
3. Příkazem `fdisk -l` zjistěte název zařízení USB flash disku (např. `/dev/sdb`).
4. Nahrajte obraz disku na USB flash disk příkazem:

   ```
   dd if=kerio-control-appliance.iso of=/dev/sdx bs=1M
   ```

   `kerio-control-appliance.iso` nahraďte skutečným názvem souboru a `/dev/sdx` skutečným zařízením. Je potřeba uvést fyzické zařízení (např. `/dev/sdx`), nikoliv oddíl (např. `/dev/sdx1`).
5. Příkazem `sync` zajistěte dokončení všech diskových operací.
6. Odpojte USB flash disk od vašeho počítače.

Mac OS X

1. Připojte USB flash disk k vašemu počítači. V případě potřeby zálohujte soubory, které jsou na něm uložené. Obsah flash disku bude kompletně přepsán!
2. Spusťte terminál (*Applications* → *Utilities* → *Terminal*).

3. Příkazem `sudo diskutil list` zjistěte název zařízení USB flash disku (např. `/dev/diskX` nebo `/dev/DiskY` — pozor na malá a velká písmena).
4. Příkazem `sudo diskutil unmountDisk /dev/diskX` disk odmountujte.
5. Nahrajte soubor obraz disku na USB flash disk příkazem:

   ```
   sudo dd if=rescue.img of=/dev/disk1 bs=1m
   ```

   `rescue.img` nahraďte skutečným názvem souboru a `/dev/diskX` skutečným zařízením.
6. Odpojte USB flash disk od vašeho počítače.

27.2 Zálohování a přenos konfigurace

V případě nutnosti přeinstalování operačního systému firewallu (např. při výměně hardware) je možné zálohovat konfiguraci *Kerio Control* včetně lokálních uživatelských účtů a (volitelně) SSL certifikátů. Tuto zálohu pak lze použít pro obnovení původní konfigurace v nové instalaci *Kerio Control*. 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 administračního rozhraní, otevřeme Konfiguračního asistenta a klikneme na příslušný odkaz.

Export konfigurace

Při exportu konfigurace bude vytvořen balík ve formátu *.tgz* (archiv *tar* komprimovaný *gzip*) obsahující všechny důležité konfigurační soubory *Kerio Control*. Volitelně mohou být do archivu přidány také SSL certifikáty WWW rozhraní, VPN serveru a serveru *SSL-VPN*. Exportovaná konfigurace neobsahuje licenčním klíč *Kerio Control*.

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 *Kerio Control* 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 7) a/nebo komunikačních pravidel (viz kapitola 9).

27.3 Konfigurační soubory

V této kapitole uvádíme přehledný popis konfiguračních a stavových souborů *Kerio Control*. 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 27.2!

Konfigurační soubory

Veškeré konfigurační informace *Kerio Control* jsou uloženy v adresáři, kde je aplikace nainstalována

(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:

sslcert
: SSL certifikáty pro všechny komponenty využívající SSL pro zabezpečení komunikace (tj. WWW rozhraní, VPN server a rozhraní *Clientless SSL-VPN*).

license
: Pokud byl *Kerio Control* již zaregistrován, obsahuje adresář `license` soubor s licenčním klíčem (i v případě registrované zkušební verze). Není-li *Kerio Control* dosud zaregistrován, pak je adresář `license` prázdný.

Stavové soubory

Kerio Control rovněž vytváří několik souborů a adresářů, do kterých ukládá určité stavové informace.

Soubory:

dnscache.cfg
: DNS záznamy uložené v cache modulu *DNS* (viz kapitola 11.1).

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 11.2).

stats.cfg
: Data statistik rozhraní (viz kapitola 22.2) a statistik uživatelů (viz kapitola 22.1).

vpnleases.cfg
: IP adresy přidělené VPN klientům (viz kapitola 25.2).

Adresáře:

logs
: Do adresáře `logs` ukládá *Kerio Control* všechny záznamy (viz kapitola 24).

star
: Adresář `star` obsahuje kompletní databázi pro statistiky zobrazované ve WWW rozhraní *Kerio Control*.

Manipulace s konfiguračními soubory

Před jakoukoliv manipulací s konfiguračními soubory (zálohováním, obnovováním apod.) je doporučeno zastavit *Kerio Control 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.

27.4 Automatické ověřování uživatelů pomocí NTLM

Kerio Control 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. Server Kerio Control musí být členem příslušné domény *Windows NT* (Windows NT Server) nebo *Active Directory* (Windows Server 2000/2003/2008).

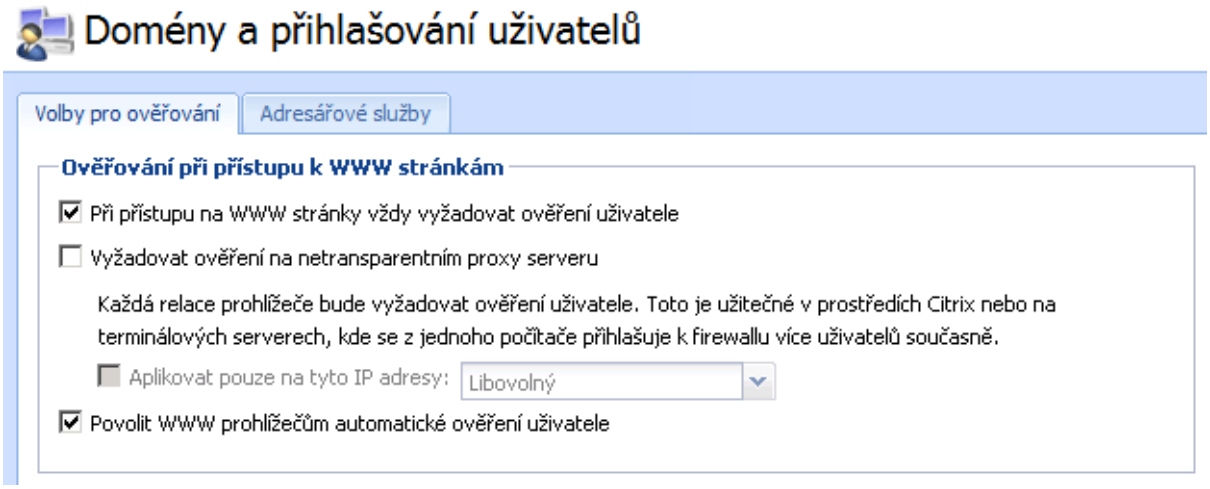
2. Příslušný uživatelský účet v Kerio Control musí být ověřován v doméně *Active Directory* nebo *Windows NT* (viz kapitola 18.1).

3. Klientský počítač musí být rovněž členem této domény.

4. Uživatel na klientském počítači se musí přihlašovat do domény (tzn. nelze použít lokální uživatelský účet).

Konfigurace Kerio Control

V sekci *Domény a přihlašování uživatelů* → *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 27.1 NTLM — nastavení ověřování uživatelů

V konfiguraci WWW rozhraní *Kerio Control* musí být nastaveno platné DNS jméno serveru *Kerio Control* (podrobnosti viz kapitola 14.1).

Obrázek 27.2 Nastavení parametrů WWW rozhraní Kerio Control

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*
- *Firefox nebo SeaMonkey*

V obou případech je potřeba v prohlížeči nastavit *Kerio Control* jako důvěryhodný server. Na nedůvěryhodných serverech nebude uživatel ověřen.

Nastavení prohlížeče Internet Explorer

- V hlavní nabídce zvolte *Nástroje* → *Možnosti Internetu*.
- V záložce *Upřesnění* v sekci *Zabezpečení* zapněte volbu *Povolit integrované ověřování systému Windows*. Zapnutí této volby vyžaduje restart prohlížeče.
- V záložce *Zabezpečení* vyberte zónu *Místní intranet*, stiskněte tlačítko *Servery* a v dalším dialogu tlačítko *Upřesnění*.
- Do seznamu důvěryhodných serverů přidejte internetové jméno serveru *Kerio Control* — např. `gw.firma.cz`. Pro zvýšení bezpečnosti můžete povolit pouze zabezpečené ověřování — pak zadejte jméno serveru ve tvaru `https://gw.firma.cz`. Server nelze zadat IP adresou!

Nastavení prohlížeče Firefox / SeaMonkey

- Do adresního řádku prohlížeče zadejte `about:config`.
- Pomocí filtru vyhledejte konfigurační parametr `network.automatic-ntlm-auth.trusted-uris`.
- Do seznamu důvěryhodných serverů zadejte (přidejte) přidejte internetové jméno serveru *Kerio Control* — např. `gw.firma.cz`. Pro zvýšení bezpečnosti můžete povolit pouze zabezpečené ověřování — pak zadejte jméno serveru ve tvaru `https://gw.firma.cz`. Server nelze zadat IP adresou!

Průběh NTLM ověření

Z pohledu uživatele probíhá NTLM ověření na firewallu zcela transparentně.

Pouze v případě, že se NTLM ověření nezdaří (např. pokud v *Kerio Control* neexistuje uživatelský účet pro uživatele přihlášeného na klientském počítači), se zobrazí přihlašovací dialog. V takovém případě se zapíší podrobné informace o nezdařeném přihlášení do záznamu *error* (viz kapitola 24.8).

Upozornění:
Jedním z důvodů selhání NTLM ověření v prohlížeči Internet Explorer může být neplatné přihlašovací jméno/heslo uložené ve *Správci hesel* systému Windows pro příslušný server Kerio Control. Prohlížeč 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 a hesla pro server, na kterém je *Kerio Control* nainstalován.

27.5 FTP přes proxy server v Kerio Control

Proxy server v aplikaci *Kerio Control* (viz kapitola 11.5) 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 v *Kerio Control*.

1. FTP klient musí umožňovat nastavení proxy serveru. Toto umožňují např. WWW prohlížeče (*Internet Explorer*, *Firefox/SeaMonkey*, *Google Chrome* 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 *Kerio Control*), 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“.

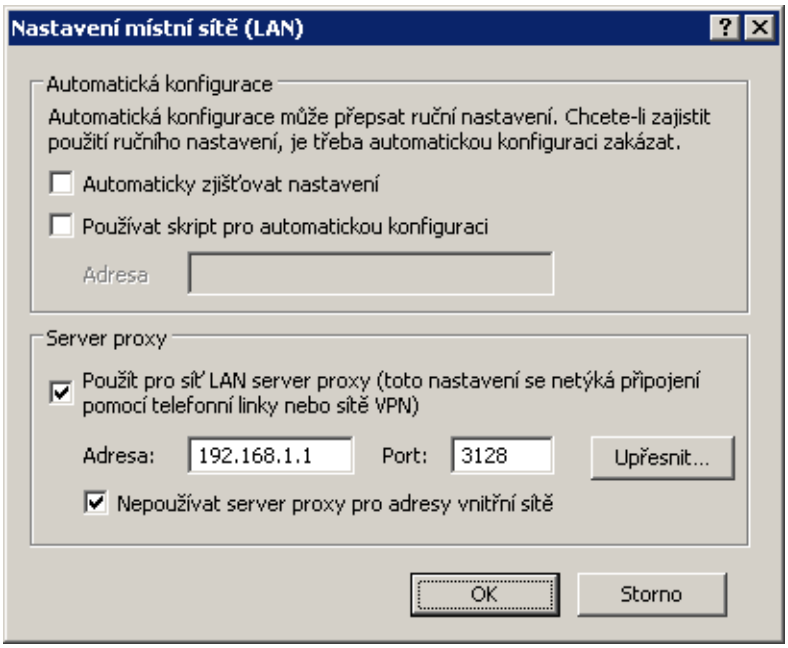
Poznámka:
FTP přes proxy server doporučujeme používat pouze v případech, kdy nelze využít přímý přístup do Internetu (viz kapitola 11.5).

Příklad konfigurace klienta: WWW prohlížeč

WWW prohlížeče umožňují nastavit proxy server buď globálně, nebo pro jednotlivé protokoly. Jako příklad uvedeme nastavení prohlížeče *Internet Explorer* (konfigurace ostatních prohlížečů je velmi podobná).

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 *Kerio Control* připojeného do lokální sítě; výchozí port proxy serveru je `3128` (podrobnosti viz kapitola 11.5). Doporučujeme zapnout rovněž volbu *Nepoužívat server proxy pro adresy vnitřní sítě* — použití proxy pro lokální servery by zbytečně zpomalovalo komunikaci a zatěžovalo *Kerio Control*.



Obrázek 27.3 Nastavení proxy serveru v prohlížeči Internet Explorer

> ***Tip***
> Pro nastavení WWW prohlížečů můžeme s výhodou využít konfigurační skript, případně automatickou detekci nastavení. Podrobnosti viz kapitola 11.5.

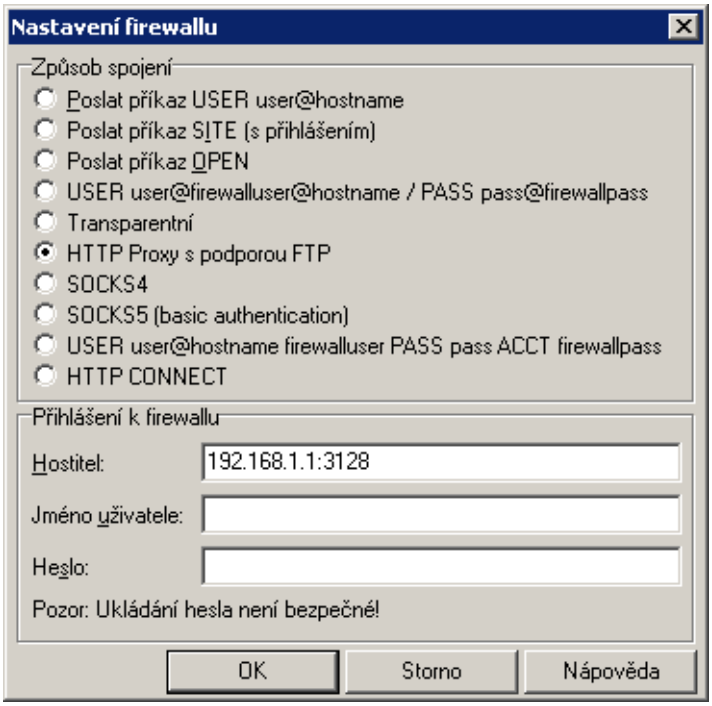
Poznámka:
WWW prohlížeče jako FTP klienti umožňují pouze download souborů. Upload na FTP server pomocí WWW prohlížeče není možný.

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 potřeba vyplňovat (*Kerio Control* s těmito údaji nepracuje).



Obrázek 27.4 Nastavení proxy serveru pro FTP v aplikaci Total Commander

> ***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.

27.6 Internetové linky vytáčené na žádost

Při použití internetové linky vytáčené na žádost (viz kapitola 8.5) 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 8.5).

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 *Kerio Control* 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, *Kerio Control* 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 Network* (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 *Kerio Control* by neměl žádný důvod vytáčet linku.
2. Pro vytáčení na žádost může být v *Kerio Control* nastavena vždy pouze jedna linka. *Kerio Control* neumožňuje automatický výběr linky, která má být vytočena.

3. Linka může být také vytáčena na základě statické cesty ve směrovací tabulce (viz kapitola 20.1). 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. *Kerio Control* 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 *Kerio Control* a vytáčené linky k Internetu.

1. Vytáčení na žádost nefunguje přímo z počítače, na němž je *Kerio Control* nainstalován. Technicky jej totiž realizuje nízkoúrovňový ovladač *Kerio Control*, 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 *Kerio Control* 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 *Kerio Control* (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 *Kerio Control*. 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* v *Kerio Control* 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 *Kerio Control*).

3. Z předchozího bodu vyplývá, že pokud má DNS server běžet přímo na počítači s *Kerio Control*, 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 *Kerio Control* nasazen na tentýž počítač, kde běží *Windows Server* s *Active Directory* a *Microsoft* DNS.

4. Je-li použit modul *DNS*, pak *Kerio Control* může za určitých okolností vytáčet i na základě požadavku přímo z počítače, na němž je nainstalován.

   Podmínkou je, že cílový server musí být zadán DNS jménem, aby byl vyslán DNS dotaz.

5. *Proxy server* v *Kerio Control* (viz kapitola 11.5) 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.

Komunikační pravidla

Je-li v komunikačních pravidlech (viz kapitola 9) zdrojový nebo cílový počítač zadán DNS jménem, pak *Kerio Control* zjišťuje odpovídající IP adresu v okamžiku stisknutí tlačítka *Použít*.

Pokud není nalezen odpovídající záznam v DNS cache, vysílá se DNS dotaz do Internetu. Pokud je internetová linka 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!

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 stačí využít tabulku jmen počítačů a/nebo tabulku přidělených adres DHCP serveru — viz kapitola 11.1).

Nežádoucí komunikaci způsobující vytáčení linky je možné v *Kerio Control* blokovat komunikačními pravidly (viz kapitola 9.3). 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 *Kerio Control* 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*).

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.

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 tabulce jmen počítačů a tabulce přidělených adres DHCP serveru v *Kerio Control*). 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).

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®, *iPad*®, *Safari*™ a *Multi-Touch*™ jsou registrované ochranné známky nebo ochranné známky společnosti *Apple Inc.*

Linux® je registrovaná ochranná známka, jejímž držitelem je Linus Torvalds.

VMware® je registrovaná ochranná známka společnosti VMware, Inc.

Mozilla® a *Firefox*® jsou registrované ochranné známky společnosti *Mozilla Foundation*.

Chrome™ je ochranná známka společnosti *Google Inc.*

Kerberos™ je ochranná známka *Massachusetts Institute of Technology* (*MIT*).

Snort® je registrovaná ochranná známka společnosti *Sourcefire, Inc.*

Sophos® je registrovaná ochranná známka společnosti *Sophos Plc.*

avast!® je registrovaná ochranná známka společnosti *AVAST Software*.

ClamAV™ je ochranná známka, jejímž držitelem je Tomasz Kojm.

ESET® a *NOD32*® jsou registrované ochranné známky společnosti *ESET, LLC.*

AVG® je registrovaná ochranná známka společnosti *AVG Technologies*.

Thawte® je registrovaná ochranná známka společnosti *VeriSign, Inc.*

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 Control* 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 *Kerio Control* pro systém 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 *GNU General Public License* verze 2.
Kompletní zdrojový kód je dostupný na adrese:

http://download.kerio.com/archive/

KIPF — API

Kerio IP filter driver for Linux API library (API knihovna síťového ovladače *Kerio Control* pro systém 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 *GNU Lesser General Public License* verze 2.

Kompletní zdrojový kód je dostupný na adrese:

http://download.kerio.com/archive/

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 *GNU General Public License* verze 2.
Kompletní zdrojový kód je dostupný na adrese:

http://download.kerio.com/archive/

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 *GNU Lesser General Public License* verze 2.
Kompletní zdrojový kód je dostupný na adrese:

http://download.kerio.com/archive/

libcurl

Copyright © 1996-2008 Daniel Stenberg.

libiconv

libiconv provádí konverze různých znakových sad prostřednictvím konverze z/do Unicode. *Kerio Control* obsahuje upravenou verzi této knihovny, která je šířena v souladu s licencí *GNU Lesser General Public License* 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.com/archive/

libmbfl

Libmbfl je knihovna pro filtrování a konverzi vícebytových znaků, distribuovaná v souladu s licencí *GNU Lesser General Public License* verze 2.
Copyright © 1998-2002 HappySize, Inc. All rights reserved.

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.

Netfilter4Win

Netfilter4win je implementace rozhraní *libnetfilter_queue* pro systém *Windows*, distribuovaná v souladu s licencí *GNU General Public License* verze 2.
Copyright © Kerio Technologies s.r.o.
Copyright © 2005 Harald Welte
Distribuční balík kompletních zdrojových kódů je k dispozici na adrese:

http://download.kerio.com/archive/

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.

Operační systém zařízení

Produkt *Kerio Control* v edicích *Appliance* a *Box* jsou založena na volně šiřitelném software z různých zdrojů. Podrobné informace o licencích veškerého použitého software jsou uvedeny v souboru

`/opt/kerio/winroute/doc/Acknowledgements`

na disku zařízení.
Distribuční balík kompletních zdrojových kódů je k dispozici na adrese:

http://download.kerio.com/archive/

PHP

Copyright © 1999-2006 The PHP Group. All rights reserved.
Tento produkt obsahuje software *PHP*, volně dostupný na adrese:

http://www.php.net/software/

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/

ScoopyNG

Nástroj pro detekci VMware.

Tento produkt obsahuje software, jehož autorem je Tobias Klein.

Snort

Snort je volně šiřitelný systém detekce a prevence síťových útoků (*IDS/IPS*). Distribuční balík obsahuje vlastní systém *Snort* a knihovny *pcre* a *pthreads-win32*. Balík je šířen jako celek v souladu s licencí *GNU General Public License* verze 2.

Distribuční balík kompletních zdrojových kódů je k dispozici na adrese:

http://download.kerio.com/archive/

zlib