

Kerio WinRoute Firewall 6

Příručka uživatele

Kerio Technologies s.r.o.

© Kerio Technologies s.r.o. Všechna práva vyhrazena.

Tento manuál popisuje uživatelská rozhraní produktu *Kerio WinRoute Firewall* ve verzi 6.7.0. Aplikace *Kerio VPN Client* je popsána v samostatném manuálu *Kerio VPN Client — Příručka uživatele*. Změny vyhrazeny.

Aktuální verzi produktu naleznete na WWW stránce

<http://www.kerio.cz/cz/firewall/download>, další dokumentaci na stránce

<http://www.kerio.cz/cz/firewall/manual>.

Informace o registrovaných ochranných známkách a ochranných známkách jsou uvedeny v příloze [A](#).

Obsah

1	Úvod	4
2	Uživatelské WWW rozhraní	5
2.1	Přístup k WWW rozhraní a ověření uživatele	5
2.2	Stavové informace a statistiky uživatele	8
2.3	Uživatelské předvolby	9
2.4	Ovládání vytáčených linek	12
3	Kerio StaR — statistiky a reportování	13
3.1	Přihlášení do StaR a zobrazení statistik	13
3.2	Nastavení reportovacího období	15
3.3	Celkový přehled	17
3.4	Statistiky uživatelů	20
3.5	Aktivita uživatelů	21
3.6	Přehled uživatelů podle objemu přenesených dat	27
3.7	Nejnavštěvovanější WWW stránky	28
3.8	Nejnavštěvovanější kategorie WWW stránek	29
4	Kerio Clientless SSL-VPN	32
4.1	Použití rozhraní SSL-VPN	32
A	Právní doložka	38
	Slovníček pojmů	39
	Rejstřík	42

Kapitola 1

Úvod

Kerio WinRoute Firewall (dále jen „*WinRoute*“, resp. „firewall“) je komplexní nástroj pro připojení lokální sítě k Internetu, zabezpečení a monitorování sítě, sledování aktivit a řízení přístupu uživatelů do Internetu. *WinRoute* nabízí také nástroje určené nejen pro správce sítě:

- Uživatelské WWW rozhraní — slouží k ověření uživatele na firewallu, zobrazení stavových informací a nastavení uživatelských předvoleb. Podrobnosti viz kapitola [2](#).
- *Kerio StaR* — zobrazuje informace o aktivitách uživatelů, navštívených WWW stránkách, objemu přenesených dat a další údaje. Podrobnosti viz kapitola [3](#).
- *Kerio SSL-VPN* — umožňuje vzdálený přístup z Internetu k souborům ve sdílených složkách na počítačích v lokální síti. Podrobnosti viz kapitola [4](#).

Ve všech případech se jedná o tzv. webová rozhraní, což znamená, že pro přístup do těchto rozhraní použijeme WWW prohlížeč, do kterého zadáme určitou specifickou adresu (URL). Pro plnou a správnou funkci je potřeba použít některý z podporovaných WWW prohlížečů:

- *Internet Explorer 6 a vyšší*
- *Firefox 1.5 a vyšší*
- *Safari*

Tato uživatelská příručka popisuje funkce jednotlivých rozhraní a možnosti jejich použití. Nezabývá se možnostmi konfigurace samotného firewallu. Obecně proto platí, že v případě nejasností či problémů je nejvhodnější kontaktovat správce příslušného firewallu.

Kapitola 2

Uživatelské WWW rozhraní

Základní funkcí WWW rozhraní *WinRoute* je přihlášení uživatele k firewallu. Firewall bývá zpravidla nastaven tak, že povoluje přístup ke službám v Internetu (WWW stránky, multimédia, FTP servery atd.) pouze přihlášeným uživatelům. Pro jednotlivé uživatele pak firewall sleduje statistiky (navštívené WWW stránky, objem přenesených dat atd.) a aplikuje případná omezení. Z důvodu jednoduchosti je zpravidla nastaveno automatické přesměrování na přihlašovací stránku WWW rozhraní, pokud uživatel přistupuje na libovolnou WWW stránku a není dosud přihlášen k firewallu. Po úspěšném přihlášení je pak prohlížeč přesměrován na požadovanou WWW stránku. Toto proběhne typicky při otevírání domovské stránky při spuštění WWW prohlížeče. Ověření uživatele na firewallu je tak téměř transparentní.

Všem uživatelům (bez ohledu na přístupová práva) WWW rozhraní umožňuje také:

- Zobrazení denní, týdenní a měsíční kvóty objemu přenesených dat a jejich aktuálního naplnění,
- Zobrazení pravidel pro omezení přístupu na WWW stránky,
- Nastavení filtrování určitých prvků WWW stránek (např. blokování vyskakovacích oken),
- Nastavení preferovaného jazyka WWW rozhraní a výstrah zasílaných e-mailem (např. o nalezeném viru nebo překročení kvóty objemu dat),
- Možnost změny hesla (pouze v některých případech).

Uživatelé s příslušnými právy mohou rovněž:

- Prohlížet statistiky využívání Internetu (viz kapitola [3](#)),
- Vytáčet a zavěšovat vytáčená internetová připojení.

2.1 Přístup k WWW rozhraní a ověření uživatele

WWW rozhraní *WinRoute* je k dispozici ve dvou verzích: nezabezpečené a zabezpečené SSL (obě verze obsahují totožné stránky).

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

`http://server:4080/`

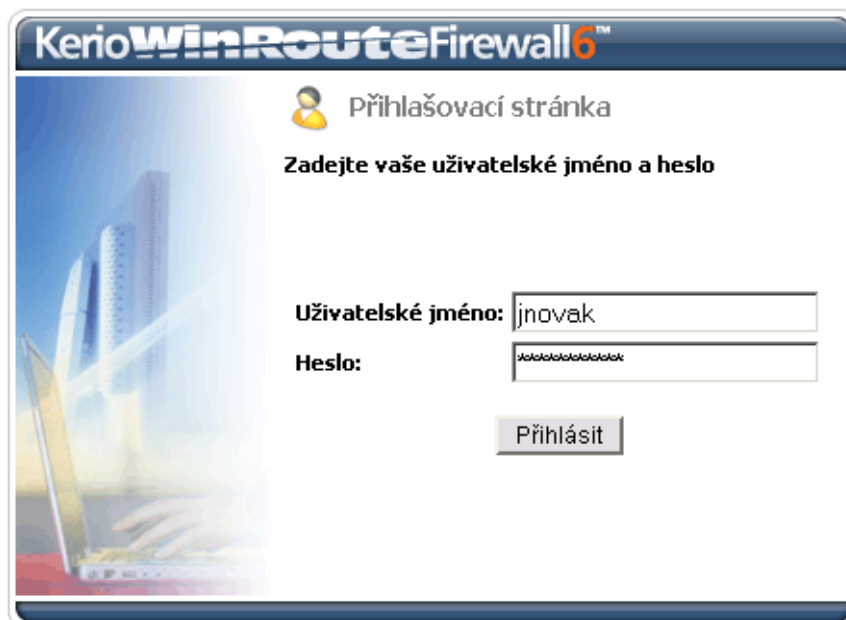
Pro zabezpečenou verzi je třeba uvést protokol HTTPS a port zabezpečeného WWW rozhraní (standardně 4081):

`https://server:4081/`

Přihlášení uživatele

Při přístupu k WWW rozhraní *WinRoute* je vyžadováno ověření uživatele. Do WWW rozhraní může přistupovat každý uživatel, který má ve *WinRoute* vytvořen uživatelský účet (bez ohledu na přístupová práva).

Pokud je počítač uživatele členem domény *Windows*, může být uživatel při přístupu k WWW rozhraní přihlášen automaticky. V opačném případě se nejprve zobrazí přihlašovací stránka firewallu s dialogem pro zadání uživatelského jména a hesla. Přihlašovací údaje jsou ve většině případů shodné jako pro přihlášení do systému na počítači uživatele.



Obrázek 2.1 Přihlašovací stránka WWW rozhraní firewallu

Upozornění

V sítích s více doménami (typicky ve velkých organizacích s několika pobočkami) může být vyžadováno zadání uživatelského jména včetně domény (např. `jnovak@pobocka.firma.cz`). Tuto informaci je nutné získat od správce příslušného firewallu.

Pokud byl uživatel na přihlašovací stránku přesměrován automaticky (zadáním URL stránky, pro niž firewall vyžaduje ověření), bude po úspěšném přihlášení přesměrován na původně požadovanou WWW stránku. V opačném případě bude zobrazena úvodní stránka WWW rozhraní.

Úvodní stránka WWW rozhraní se liší podle práv přihlášeného uživatele:

- Má-li uživatel právo prohlížet statistiky, pak bude WWW rozhraní přepnuto do režimu *Kerio StaR* a jako úvodní stránka se zobrazí souhrnné statistiky (záložka *celkově* —

podrobnosti viz kapitola 3). Volbou *Můj účet* v pravém horním rohu stránky se lze přepnout na uživatelská nastavení a volbou *Statistiky* zpět na statistiky.

- Není-li uživatel oprávněn prohlížet statistiky, pak se jako úvodní stránka zobrazí stavové informace o daném uživateli (viz kapitola 2.2).

Odhlášení uživatele

Po skončení činnosti, která vyžadovala ověření uživatele, by se uživatel měl od firewallu odhlásit prostřednictvím odkazu *Odhlásit* v pravém horním rohu stránky WWW rozhraní. Odhlášení je důležité zejména v případech, kdy na jednom počítači pracuje střídavě více uživatelů. Kdyby se jeden uživatel od firewallu neodhlásil, další by pak mohli pracovat bez přihlášení pod jeho identitou.

Uživatel může být na firewallu přihlášen, i když nepracoval s WWW rozhraním — např. firewall vyžadoval ověření uživatele při přístupu na WWW stránku. Aby uživatel v takových případech nemusel po skončení práce otevírat WWW rozhraní a následně klikat na odkaz *Odhlásit*, nabízí *WinRoute* také přímý odkaz pro odhlášení uživatele:

`http://server:4080/logout`

resp.

`https://server:4081/logout`

Při přístupu na toto URL dojde k okamžitému odhlášení uživatele bez nutnosti zobrazování úvodní stránky WWW rozhraní.

Tip

URL pro odhlášení od firewallu můžeme přidat jako odkaz do nástrojového pruhu WWW prohlížeče. Uživatel tak bude mít stále k dispozici „tlačítko“ pro snadné odhlášení od firewallu.

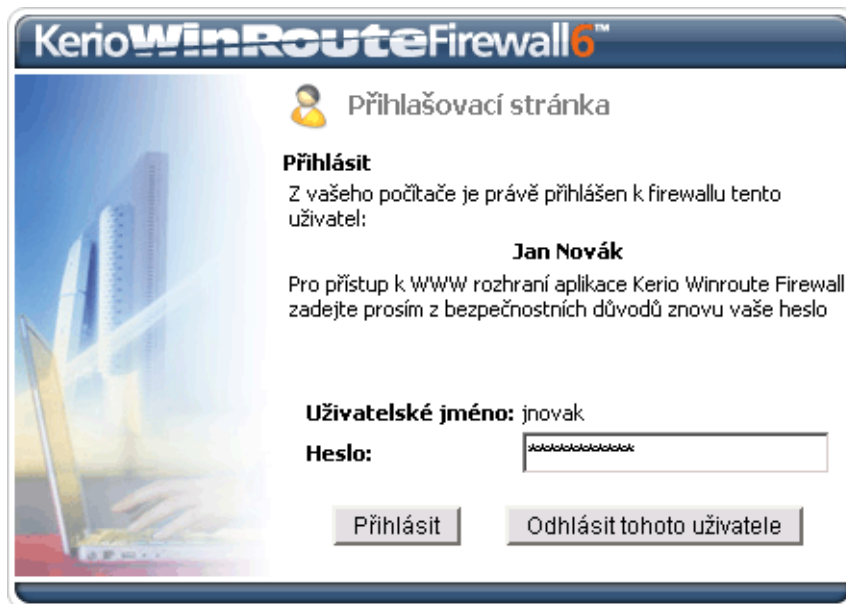
Poznámka: *WinRoute* rovněž umožňuje automatické odhlášení při nečinnosti — pokud uživatel nevyužívá žádnou internetovou službu po stanovenou dobu (standardně 2 hodiny), pak je od firewallu automaticky odhlášen. Tím jsou ošetřeny případy, kdy se uživatel zapomene sám odhlásit.

Ověření hesla uživatele

Pokud přistupujeme na WWW rozhraní v době, kdy je přihlášení uživatele z daného počítače dosud platné (tzn. uživatel se neodhlásil ani nevypršela doba nečinnosti, ale příslušná relace prohlížeče¹ již vypršela, pak *WinRoute* požaduje ověření uživatele zadáním jeho hesla. Hlavním důvodem pro toto znovuověření je potenciální možnost zneužití identity přihlášeného uživatele jiným uživatelem.

Za uvedených podmínek se v prohlížeči zobrazí speciální verze přihlašovací stránky.

¹ *Relace* (angl. *session*, někdy též překládáno jako *sezení*) je období běhu jedné instance prohlížeče. Např. v případě prohlížečů *Internet Explorer*, *Firefox* nebo *Opera* relace zaniká po uzavření všech otevřených oken prohlížeče, zatímco u prohlížeče *SeaMonkey* relace zaniká až po ukončení programu *Rychlé spuštění* (ikona v oznamovací oblasti nástrojové lišty).



Obrázek 2.2 Ověření hesla přihlášeného uživatele

Pokud k WWW rozhraní přistupuje tentýž uživatel, který je již přihlášen, může se ověřit zadáním svého hesla a pokračovat v práci s WWW rozhraním. Pokud WWW rozhraní otevřel jiný uživatel, musí aktuálního uživatele nejprve odhlásit a poté se ověřit svým vlastním uživatelským jménem a heslem.

2.2 Stavové informace a statistiky uživatele

V záložce *Stav* jsou zobrazovány tyto údaje:

Informace o uživateli a firewallu

V záhlaví stránky se zobrazuje celé jméno nebo uživatelské jméno a DNS jméno nebo IP adresa firewallu.

Statistika kvóty objemu dat

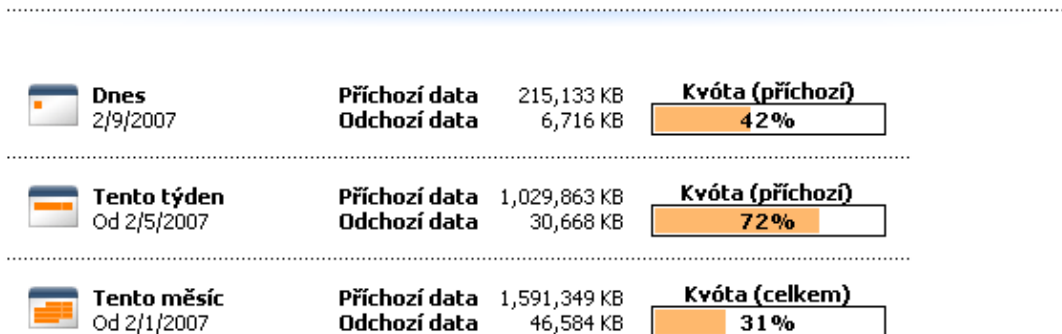
Horní část záložky *Stav* zobrazuje aktuální objem přenesených dat v příchozím směru (download) a odchozím směru (upload) za dnešní den, tento týden a tento měsíc. Je-li nastavena některá kvóta, pak je zde zobrazeno také aktuální využití jednotlivých kvót (v procentech).

Tip

Začátek týdne a začátek měsíce lze ovlivnit nastavením tzv. účtovacího období v konfiguraci *WinRoute*.




Aktuální omezení přístupu na WWW stránky

Dolní část záložky *Stav* zobrazuje aktuální pravidla pro URL, která jsou na daného uživatele aplikována (tzn. pravidla platná buď pro všechny uživatele nebo přímo pro tohoto uživatele nebo pro skupinu, do níž tento uživatel náleží). Uživatel tak může snadno zjistit, k jakým WWW stránkám a typům objektů má povolen přístup a k jakým nikoliv. Zobrazuje se i časová platnost jednotlivých pravidel.

 Statistika kvóty objemu přenesených dat


Obrázek 2.3 Statistika kvóty objemu dat

 Omezení přístupu na WWW stránky

URL	Povoleno	Typ obsahu	Časový interval
.kerio.com	 Ano	Libovolný	Libovolný
.ads. */ad/* *adframe* */ad-handler/* */ads/* */banner/* */please/showit* */popup/* */popups/* *.gator.com* *adserv* ad.* ad?.* ad??.* ad???.* ads???.*	 Ne	Libovolný	Libovolný
.windowsupdate.com/ *update.microsoft.com/*	 Ano	Libovolný	Libovolný

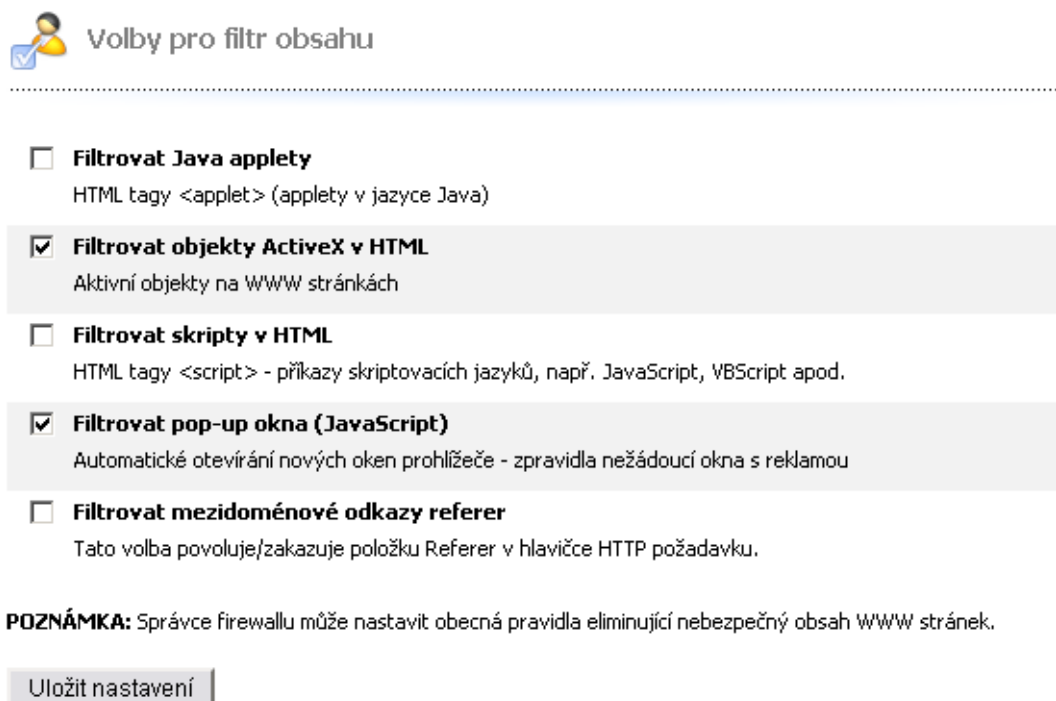
Obrázek 2.4 Aktuální pravidla pro přístup na WWW stránky

2.3 Uživatelské předvolby

V záložce *Předvolby* si může každý uživatel nastavit vlastní podmínky filtrování obsahu WWW stránek a preferovaný jazyk, ve kterém bude WWW rozhraní zobrazováno. Pokud uživatel nepoužívá účet z domény *Windows*, pak si v předvolbách může také změnit své heslo.

Volby pro filtrování obsahu WWW stránek

Horní část záložky umožňuje povolit či zakázat určité prvky v HTML stránkách.



Obrázek 2.5 Uživatelské nastavení filtrování objektů na WWW stránkách

Volby pro filtrování obsahu

Zaškrtnutí políčka pod názvem prvku znamená, že tento prvek bude filtrován firewallem. Je-li určitý prvek zakázán správcem *WinRoute*, pak je příslušné pole na této stránce neaktivní — uživatel nemůže nastavení změnit. Uživatel smí svá pravidla pouze zpřísnit — nemůže povolit HTML prvek, který mu zakázal správce *WinRoute*.

- *Java applety* — blokování HTML tagů `<applet>`
- *ActiveX* — prvky *Microsoft ActiveX* (tato technologie dovoluje mimo jiné např. spouštění aplikací na klientském počítači).
Tato volba blokuje HTML tagy `<object>` a `<embed>`.
- *Skripty* — blokování HTML tagů `<script>` (příkazy jazyků JavaScript, VBScript atd.)
- *Pop-up okna* — automatické otevírání nových oken prohlížeče — typicky reklamy.
Tato volba blokuje ve skriptech v jazyce *JavaScript* metodu `window.open()`.
- *Cross-domain referer* — blokování položek *Referer* v HTTP hlavičce.
Tato položka obsahuje URL stránky, z níž klient na danou stránku přešel. Volba *Cross-domain referer* blokuje položku *Referer* v případě, že obsahuje jiné jméno serveru než aktuální požadavek.
Blokování *Cross-domain referer* má význam pro ochranu soukromí uživatele (položka *Referer* může být sledována pro zjištění, jaké stránky uživatel navštívuje).

Uložit nastavení

Stisknutím tohoto tlačítka se nastavené volby uloží a aktivují.

Změna uživatelského hesla

Střední část záložky *Předvolby* slouží pro změnu hesla uživatele. Změna hesla není možná, pokud je uživatel přihlášen pod účtem z domény *Windows* (v takovém případě se sekce *Změna hesla* nezobrazí).

Obrázek 2.6 Změna uživatelského hesla

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

Preferovaný jazyk

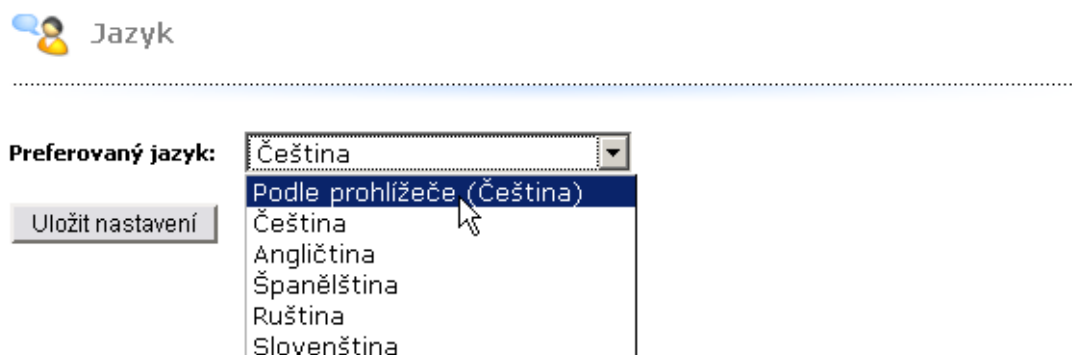
V dolní části záložky *Předvolby* si uživatel může nastavit svůj preferovaný jazyk. Tento jazyk pak bude použit pro:

- WWW rozhraní firewallu,
- *Kerio StaR*,
- Výstrahy a další informace zasílané uživateli e-mailem (např. upozornění na virus nebo překročení kvóty objemu přenesených dat).

Nastavení preferovaného jazyka se nepoužívá pro rozhraní *Kerio Clientless SSL-VPN*, ve kterém je vždy jazyk nastaven automaticky podle preferencí WWW prohlížeče.

Aktuální verze *WinRoute* nabízí výběr ze 16 jazyků. Jazyk si může uživatel vybrat ze seznamu nebo může být nastaven automaticky podle jazykových preferencí ve WWW prohlížeči klienta (výchozí volba). Tato možnost existuje ve všech podporovaných WWW prohlížečích. Není-li k dispozici žádný z jazyků preferovaných v prohlížeči, použije se výchozí — angličtina.

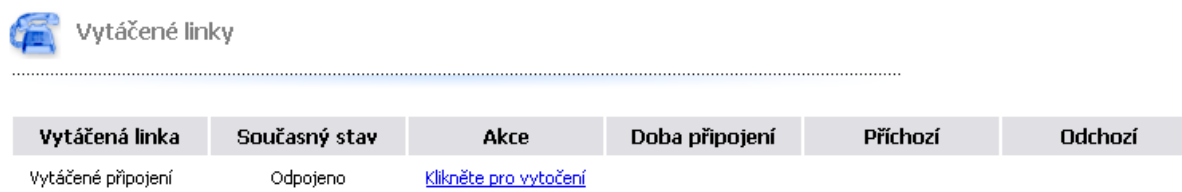
Poznámka: Nastavení jazyka ovlivňuje také formát zobrazování data a číselných údajů.



Obrázek 2.7 Nastavení preferovaného jazyka WWW rozhraní

2.4 Ovládání vytáčených linek

Pokud má uživatel právo ovládat vytáčené linky ve *WinRoute*, pak může v záložce *Vytáčené linky* vytáčet a zavěšovat jednotlivé RAS linky a sledovat jejich stav. Tato záložka zobrazuje seznam všech vytáčených linek, které jsou ve *WinRoute* definovány.



Tato stránka je automaticky obnovována.

Obrázek 2.8 WWW rozhraní — ovládání vytáčených linek

Pro každou linku jsou zobrazeny tyto údaje:

- Název linky ve *WinRoute*.
- Aktuální stav — *Odpojeno*, *Připojuje se...* (probíhá vytáčení), *Připojeno*, *Odpojuje se* (probíhá zavěšování).
- Akce — hypertextový odkaz pro vytočení nebo zavěšení linky (v závislosti na jejím aktuálním stavu).
- Doba, po kterou je linka připojena.
- Objem přenesených dat v každém směru (*příchozí* = z Internetu do lokální sítě, *odchozí* = z lokální sítě do Internetu).

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

Kerio StaR — statistiky a reportování

WinRoute poskytuje prostřednictvím WWW rozhraní podrobné statistické informace o uživateli, objemu přenesených dat, navštívených WWW stránkách a kategoriích stránek. Tyto informace lze využít např. pro sledování pracovních a nepracovních aktivit jednotlivých uživatelů.

Statistiky sledují komunikaci mezi lokální sítí a Internetem. Objemy dat přenesených mezi počítači v lokální síti a navštívené stránky na lokálních serverech nejsou do statistik zahrnovány (ani to není technicky možné).

Výhodou webových statistik a reportů je jejich snadná dostupnost. Uživatel (typicky vedoucí pracovník) nepotřebuje program *Administration Console* a nemusí mít práva ke správě *WinRoute* (přístup ke statistikám je řízen speciálním právem). Statistiky zobrazené ve webovém prohlížeči je možné i vytisknout nebo uložit na disk jako WWW stránku.

Poznámka:

1. Uživatelé by měli být informováni o tom, že jejich aktivita je na firewallu sledována.
2. Statistiky a reporty ve *WinRoute* mají informativní charakter. Nedoporučujeme je používat např. pro přesné rozúčtování nákladů na internetové připojení na jednotlivé uživatele.

3.1 Přihlášení do StaR a zobrazení statistik

K prohlížení statistik je třeba se přihlásit do WWW rozhraní *WinRoute*. Uživatel (resp. skupina, do které je zařazen) musí mít právo prohlížet statistiky. Podrobnosti o přihlašování do WWW rozhraní *WinRoute* viz kapitola [2.1](#).

Přístup ke statistikám

Z libovolného počítače, ze kterého je povolen přístup k WWW rozhraní *WinRoute*, je možné otevřít *Kerio StaR* těmito způsoby:

- Na adrese `https://server:4081/star` nebo `http://server:4080/star`. Toto je URL určené výhradně pro přístup ke *StaR*. Pokud uživatel nemá právo prohlížet statistiky, zobrazí se chybové hlášení.
- Na adrese `https://server:4081/`, resp. `http://server:4080/`. Toto je základní URL WWW rozhraní *WinRoute*. Pokud má uživatel právo prohlížet statistiky, zobrazí se úvodní stránka *StaR* s celkovými statistikami (viz níže). V opačném případě se zobrazí stránka *Můj účet*, která je dostupná všem uživatelům.

Upozornění

Při přístupu z Internetu (tj. z počítače mimo lokální síť) bude pravděpodobně dostupné pouze zabezpečené WWW rozhraní. Povolení přístupu z Internetu k nezabezpečenému WWW rozhraní by představovalo značné bezpečnostní riziko.

Stránka StaR ve WWW rozhraní

Stránka statistik je rozdělena formou záložek na tyto sekce:

- *Celkově* — souhrnný přehled komunikace za všechny uživatele v lokální síti (objemy přenesených dat, nejaktivnější uživatelé, nejnavštěvovanější WWW stránky...). Tato sekce se zobrazuje jako úvodní stránka bezprostředně po úspěšném přihlášení uživatele.
- *Uživatelé* — statistiky za jednotlivé uživatele (objemy přenesených dat, nejnavštěvovanější WWW stránky atd. pro vybraného uživatele).
- *Aktivita uživatelů* — podrobné informace o aktivitě jednotlivých uživatelů (navštívené WWW stránky, soubory přenášené FTP, multimédia, vzdálený přístup na jiné počítače atd.).
- *Komunikace uživatelů* — tabulka a graf objemů dat přenesených jednotlivými uživateli.
- *Navštívené stránky* — přehled deseti nejnavštěvovanějších WWW domén. Pro každou doménu je zobrazen graf a tabulka uživatelů, kteří navštívili nejvíce WWW stránek z dané domény.
- *Kategorie stránek* — přehled deseti nejnavštěvovanějších kategorií WWW stránek (dle kategorizace modulem *Kerio Web Filter*). Pro každou kategorii je zobrazen graf a tabulka uživatelů, kteří měli nejvíce požadavků na stránky dané kategorie.

Jednotlivé sekce jsou podrobně popsány v následujících kapitolách.

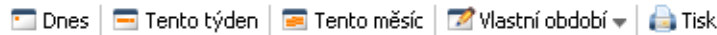
Aktualizace dat v rozhraní StaR

Rozhraní *StaR* je primárně určeno pro vytváření statistik a přehledů za určité období. Při sledování a vyhodnocování informací pro *StaR* musí *WinRoute* zpracovat poměrně velké množství dat. Aby nedocházelo k příliš velkému zatěžování firewallu (a zpomalování internetového připojení), aktualizují se data pro *StaR* vždy cca 1x za hodinu. V pravém horním rohu každé stránky rozhraní *StaR* je vždy uvedena informace o tom, kdy proběhla poslední aktualizace těchto dat.

Z výše uvedených důvodů není rozhraní *StaR* vhodné pro sledování aktivity uživatelů v reálném čase.

Formátování pro tisk

Libovolnou stránku zobrazenou v rozhraní *StaR* je možné převést do formátu vhodného pro tisk na tiskárně. K tomuto účelu slouží „tlačítko“ *Tisk* v horním nástrojovém pruhu.



Obrázek 3.1 Kerio StaR — nástrojový pruh

Po kliknutí na „tlačítko“ *Tisk* se aktuální stránka rozhraní *StaR* zobrazí v novém okně (resp. záložce) prohlížeče ve formátu vhodném pro tisk na tiskárně a otevře se dialog prohlížeče pro tisk. Velikost a stránkování jsou optimalizovány pro oba nejrozšířenější formáty papíru — A4 a Letter.

Upozornění

Z technických důvodů nelze pro tisk stránek rozhraní *StaR* použít příkaz *Soubor* → *Tisk* (resp. kombinaci kláves *Ctrl+P*). Tímto způsobem by byla vytisknuta původní (neupravená) stránka.

3.2 Nastavení reportovacího období

Při prohlížení statistik nás zpravidla zajímají pouze údaje pro určitý časový úsek (dnešní den, minulý týden apod.). Tento časový úsek se nazývá *reportovací období*.

Požadované reportovací období lze nastavit pomocí nástrojového pruhu v horní části stránky *Kerio StaR*.



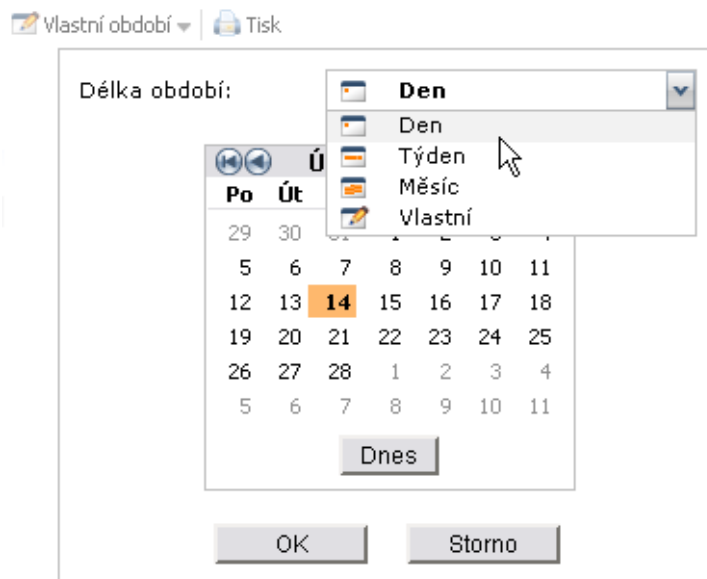
Obrázek 3.2 Kerio StaR — nástrojový pruh a reportovací období

Nástrojový pruh obsahuje tlačítka pro rychlý výběr aktuálního období (den, týden, měsíc). Šipky vedle data (aktuálního období) umožňují rychlé přepnutí na předchozí nebo následující období zvolené délky. Rychlé přepnutí není možné, pokud je zvoleno vlastní období určené počátečním a koncovým datem.

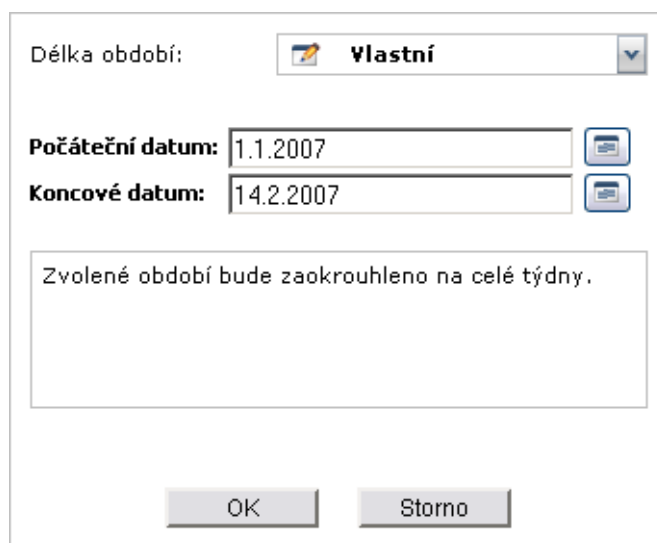
K nastavení libovolného jiného reportovacího období slouží tlačítko *Vlastní období* v horní části stránky statistik.

V položce *Délka období* lze vybrat období pevné délky (den, týden nebo měsíc). Podle zvolené délky období se zobrazí kalendář umožňující výběr roku, týdne nebo měsíce.

Poznámka: Týdny a měsíce pro účely statistik nemusí odpovídat kalendářním týdnům a měsícům. V konfiguraci statistik ve *WinRoute* lze nastavit tzv. účtovací období — začátek měsíce a první den v týdnu (případná změna účtovacího období bude mít vliv pouze na nová data, neovlivní data, která jsou již uložena v databázi).



Obrázek 3.3 Výběr reportovacího období pro zobrazení statistik



Obrázek 3.4 Nastavení vlastního reportovacího období

Další možností je definovat libovolné vlastní období určené počátečním a koncovým datem.

Počáteční i koncové datum je možné zadat ručně nebo vybrat z kalendáře (kliknutím na ikonu vedle příslušné položky).

Zvolené období platí pro statistiky ve všech záložkách a je platné až do další změny období (resp. do ukončení práce s rozhraním *Kerio StaR*). Po přihlášení do *Kerio StaR* rozhraní je vždy nastaveno výchozí období „dnešní den“.

Poznámka: Za určitých okolností může být zobrazena informace, že zvolené období bude zaokrouhleno na celé týdny nebo celé měsíce. V takovém případě se po potvrzení výběru nastaví výsledné (zaokrouhlené) období, pro které budou statistiky zobrazeny.

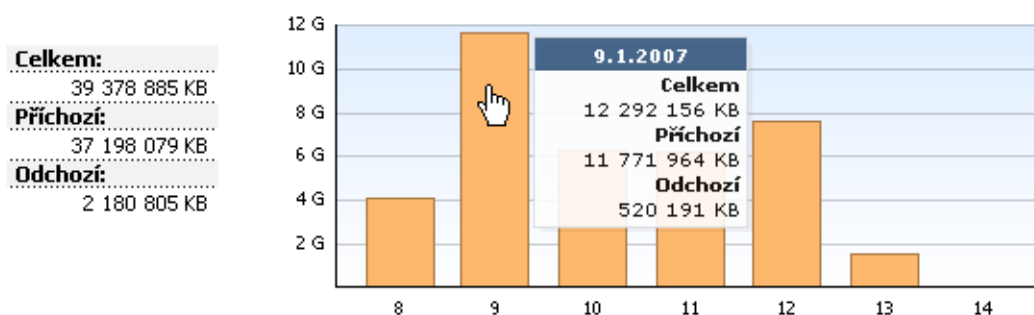
3.3 Celkový přehled

Záložka *Celkově* poskytuje souhrnné statistiky za všechny uživatele v lokální síti (včetně anonymních nepřihlášených uživatelů) ve zvoleném reportovacím období.

Komunikace po ...

První graf zobrazuje objem přenesených dat v jednotlivých podobdobích zvoleného období. Vlevo od grafu jsou uvedeny objemy přenesených dat za celé zvolené období (celkově a v každém směru). Při umístění kurzoru myši na některý sloupec grafu se zobrazí objemy přenesených dat za příslušné podobdobí. Kliknutím na sloupec grafu se reportovací období přepne na vybrané podobdobí a všechny statistiky budou zobrazeny pouze pro toto podobdobí² (viz kapitola 3.2).

● Komunikace po dnech



Obrázek 3.5 Graf komunikace po dnech

Délka podobdobí závisí na zvoleném období, pro které se statistiky zobrazují:

- *den* — graf zobrazuje komunikaci po hodinách,
- *týden* nebo *měsíc* — komunikace po dnech.

V případě vlastního období:

- *do 2 dnů (včetně)* — komunikace po hodinách,
- *do 5 týdnů* — komunikace po dnech,
- *do 6 měsíců* — komunikace po týdnech,
- *více než 6 měsíců* — komunikace po měsících.

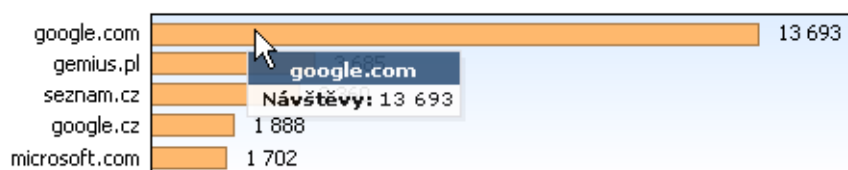
Nejnavštěvovanější WWW stránky

Graf nejnavštěvovanějších WWW stránek zobrazuje prvních pět domén (druhé úrovně) dle návštěvnosti WWW stránek. Číselný údaj v grafu znamená počet návštěv všech WWW stránek z příslušné domény v daném reportovacím období.

Poznámka: WinRoute „vidí“ pouze jednotlivé HTTP požadavky. Pro zjištění počtu návštěv stránek (tj. vyhodnocení, které požadavky byly vyslány v rámci jedné návštěvy) se používá speciální heuristický algoritmus. Z tohoto důvodu nejsou údaje o počtu návštěv absolutně přesné, jedná se však o velmi dobrou aproximaci.

² Přepnutí reportovacího období na vybrané podobdobí není možné, pokud je zobrazena komunikace po hodinách. Nejkratší možné reportovací období je 1 den.

● Nejnavštěvovanější WWW stránky

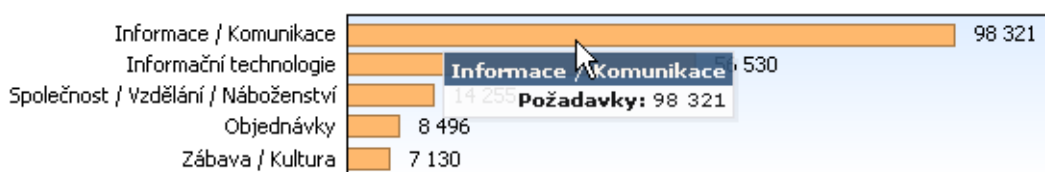


Obrázek 3.6 Graf nejnavštěvovanějších webových domén

Nejnavštěvovanější kategorie stránek

Tento graf zobrazuje pět nejžádanějších kategorií WWW stránek v daném období dle hodnocení modulem *Kerio Web Filter*. Číselný údaj v grafu znamená absolutní počet HTTP požadavků zařazených do dané kategorie. Technicky není možné rozlišit, zda se jedná o požadavky při načítání jedné stránky nebo požadavky na různé stránky. Z tohoto důvodu jsou počty požadavků zpravidla výrazně vyšší než počty návštěv WWW stránek v předchozím grafu.

● Nejnavštěvovanější kategorie stránek



Obrázek 3.7 Graf nejnavštěvovanějších kategorií WWW stránek

Prvních 5 uživatelů

Přehled pěti nejaktivnějších uživatelů, tj. uživatelů s největším celkovým objemem přenesených dat v daném reportovacím období.

Tabulka obsahuje jednotlivé uživatele a příslušný celkový objem přenesených dat.

Graf zobrazuje podíly těchto nejaktivnějších uživatelů na celkovém objemu přenesených dat v daném období. Při umístění kurzoru myši nad jméno vybraného uživatele se zobrazí objem dat přenesený tímto uživatelem celkem, v příchozím směru (download) a v odchozím směru (upload).

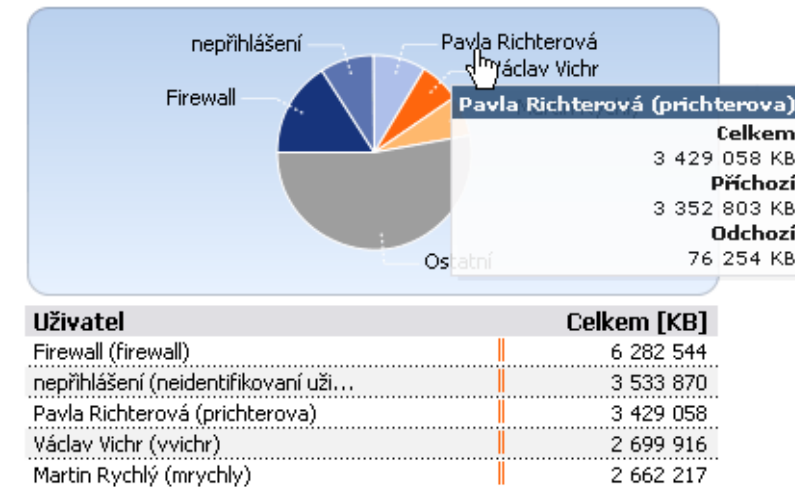
Kliknutím na jméno uživatele v grafu nebo v tabulce dojde k přepnutí do záložky *Uživatelé* (viz kapitola 3.4) a zobrazí se statistiky příslušného uživatele.

Na základě těchto informací můžeme např. zjistit, kteří uživatelé nejvíce zatěžují internetovou linku, a aplikovat na tyto uživatele příslušná omezení.

Poznámka:

1. Objem přenesených dat konkrétního uživatele je dán součtem objemů dat přenesených tímto uživatelem ze všech počítačů, ze kterých se během daného reportovacího období přihlásil k firewallu.
2. Data přenesená všemi nepřihlášenými uživateli se sčítají a zobrazují jako jedna položka (*nepřihlášení*). Tento údaj však nemá příliš velkou vypovídací hodnotu, a proto doporučujeme nastavit firewall tak, aby vždy vyžadoval přihlášení uživatele.
3. Způsob zobrazení uživatelského jména v tabulce lze nastavit v konfiguraci *WinRoute*.

● Prvních 5 uživatelů



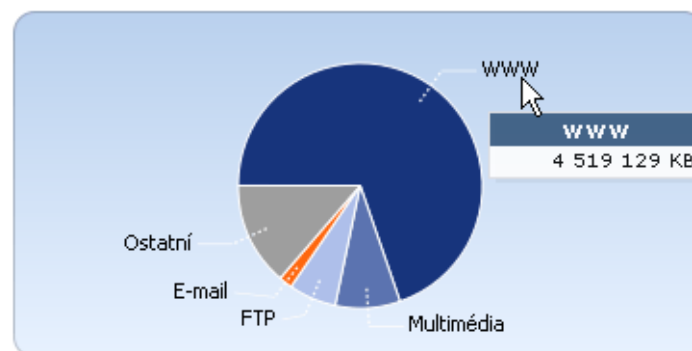
Obrázek 3.8 Statistika prvních 5 uživatelů

V grafu je vždy zobrazováno pouze celé jméno uživatele (případně uživatelské jméno, pokud není celé jméno v uživatelském účtu vyplněno).

Používané protokoly

Graf používaných protokolů zobrazuje podíl jednotlivých protokolů (resp. tříd protokolů) na celkovém objemu přenesených dat v daném reportovacím období. Při umístění kurzoru myši na název protokolu se zobrazí objem dat přenesený tímto protokolem. Tyto informace mohou být užitečné např. pro zjištění charakteru komunikace mezi lokální sítí a Internetem. Pokud je internetová linka přetěžována, můžeme na základě těchto informací aplikovat příslušná omezení (komunikační pravidla, pravidla pro URL atd.).

● Používané protokoly



Obrázek 3.9 Podíl jednotlivých protokolů na objemu přenesených dat

Z důvodu přehlednosti statistik rozlišuje *WinRoute* pouze několik předdefinovaných tříd protokolů:

- *WWW* — protokoly *HTTP*, *HTTPS* a veškerá další komunikace obsluhovaná inspekčním modulem protokolu *HTTP*,
- *E-mail* — protokoly *SMTP*, *IMAP*, *POP3* (a jejich zabezpečené verze),

- *FTP* — protokol *FTP* (včetně komunikace přes proxy server),
- *Multimédia* — protokoly pro přenos zvuku a videa v reálném čase (např. *RTSP*, *MMS*, *RealAudio*),
- *P2P* — protokoly sítí pro sdílení souborů (*peer-to-peer* — např. *DirectConnect*, *BitTorrent*, *eDonkey* apod.). Příslušná komunikace je do statistik započítávána pouze v případě, kdy *WinRoute* detekuje, že se jedná o komunikaci v *P2P* síti.
- *VPN* — připojení ke vzdáleným privátním sítím (např. *Kerio VPN*, *Microsoft PPTP* apod.).
- *Vzdálený přístup* — „terminálové“ připojení ke vzdáleným počítačům (např. *Vzdálená plocha*, *VNC*, *Telnet* nebo *SSH*).
- *Rychlé zasílání zpráv (Instant Messaging)* — online komunikace mezi uživateli pomocí služeb jako *ICQ*, *MSN Messenger*, *Yahoo! Messenger* apod.
- *Ostatní* — veškerá komunikace, která nespadá do výše uvedených kategorií.

Poznámka:


1. Pokud se namísto některého grafu zobrazí text *Data nejsou k dispozici*, znamená to, že v databázi *WinRoute* nejsou uložena žádná data pro příslušnou statistiku a vybrané reportovací období. Tento stav může mít několik různých příčin — např. zvolený uživatelský účet v daném období ještě neexistoval nebo již neexistoval, uživatel se v tomto období vůbec nepřihlásil k firewallu apod.
2. *WinRoute* se snaží optimalizovat velikost databáze statistik a objem zpracovávaných dat. Největší objem dat představují statistiky navštívených WWW stránek. Z toho důvodu se denní statistiky WWW stránek uchovávají pouze za posledních 40 dnů. Týdenní a měsíční statistiky jsou k dispozici za celou dobu uchování dat (standardně 2 roky).


Pokud je zvoleno období, pro které nejsou k dispozici potřebná data pro statistiku navštívených WWW stránek, *WinRoute* se pokusí nabídnout volbu jiného časového období, ve kterém by mohla být k dispozici data pro požadovanou statistiku.

● Nejnavštěvovanější WWW stránky

Požadovaná data nejsou k dispozici pro zvolené časové období.

Zvolte prosím jiné časové období, které (částečně) pokrývá požadované období:

 1.2.2007 - 28.2.2007

 12.2.2007 - 18.2.2007

Obrázek 3.10 Výběr jiného časového období pro statistiku WWW stránek

3.4 Statistiky uživatelů

Záložka *Uživatelé* umožňuje zobrazit statistiky pro vybraného uživatele.

Nejprve je třeba zvolit uživatelský účet v položce *Vybrat uživatele*. Tato položka obsahuje všechny uživatele, pro které jsou v databázi k dispozici nějaká statistická data — tzn. uživatelé, kteří v době sledování statistik vykazovali nějakou internetovou aktivitu.



Obrázek 3.11 Výběr uživatele pro zobrazení statistik

Tip

Způsob zobrazování uživatelského jména lze nastavit v konfiguraci *WinRoute*.

Po výběru uživatele se zobrazí jeho celé jméno, uživatelské jméno a e-mailová adresa (celé jméno a e-mailová adresa pouze v případě, že jsou tyto položky v uživatelském účtu vyplněny). Odkaz *Zobrazit aktivitu uživatele* přepne rozhraní *StaR* na stránku *Aktivita uživatelů*, kde budou zobrazeny podrobné informace o aktivitě vybraného uživatele ve zvoleném časovém období (podrobnosti viz kapitola 3.5).

Pro vybraného uživatele budou zobrazeny stejné statistiky jako v záložce *Uživatelé* pro všechny uživatele, tj.:

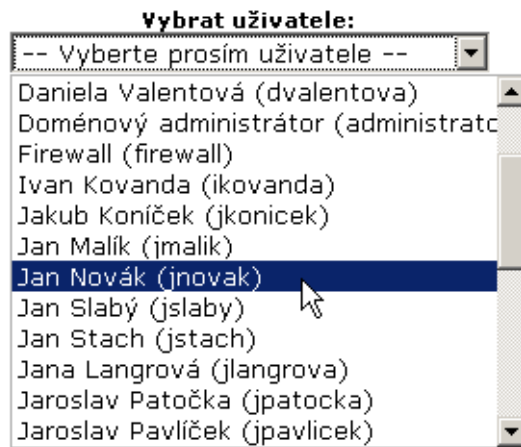
- objem přenesených dat v jednotlivých podobdobích zvoleného reportovacího období,
- nejnavštěvovanější WWW stránky,
- nejnavštěvovanější kategorie WWW stránek,
- používané protokoly a jejich podíl na celkovém objemu přenesených dat.

Podrobné informace k jednotlivým statistikám naleznete v kapitole 3.3.

3.5 Aktivita uživatelů

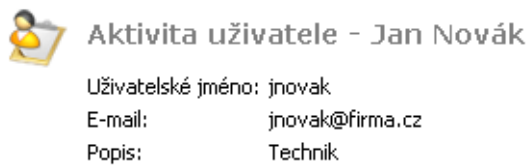
Záložka *Aktivita uživatelů* umožňuje zobrazit velmi podrobné informace o „internetové aktivitě“ jednotlivých uživatelů. Tato sekce dává odpovědi na otázky typu *Co dělal tento uživatel v daném období na Internetu? Kolik času strávil tento uživatel brouzdáním po WWW stránkách?* apod.

V pravé horní části záložky *Aktivita uživatelů* musíme nejprve vybrat uživatele, jehož aktivitu chceme zobrazit.



Obrázek 3.12 Výběr uživatele pro zobrazení aktivity

V levém horním rohu stránky pak bude zobrazeno záhlaví se všemi dostupnými informacemi o vybraném uživateli (uživatelské jméno, e-mailová adresa atd.).



Obrázek 3.13 Aktivita uživatele — informace o uživateli

Pod záhlavím je zobrazen přehled všech rozpoznaných aktivit vybraného uživatele v daném období. Neexistují-li pro toto období žádné záznamy o aktivitě vybraného uživatele, zobrazí se hlášení *Data nejsou k dispozici*. Technicky není možné rozlišit, zda uživatel neměl v daném období žádnou aktivitu nebo zda aktivitu měl, ale z nějakého důvodu nebyla zaznamenána.

Poznámka:

1. Sekce *Aktivita uživatelů* dává přehled o aktivitě uživatele za určité období, není však určena pro sledování aktivity v reálném čase. Detekované aktivity se vždy zobrazují s určitým zpožděním, které je dáno zejména dvěma faktory:
 - *Aktualizace dat v rozhraní StaR* — při sledování a vyhodnocování informací pro rozhraní *StaR* musí *WinRoute* zpracovat poměrně velké množství dat. Aby nedocházelo k příliš velkému zatěžování firewallu, aktualizují se data pro rozhraní *StaR* vždy cca 1x za hodinu (viz informace o poslední aktualizaci dat).
 - *Prodleva při zaznamenávání aktivit* — každá aktivita je zaznamenána až 15 minut poté, co byla ukončena. Důvodem je slučování bezprostředně následujících aktivit stejného typu do jednoho záznamu (pro přehlednější zobrazení aktivity uživatele).
2. Aktivitu uživatele lze zobrazit nejvýše za 7 dní (z důvodu přehlednosti). Je-li zvoleno delší časové období, budou uživateli nabídnuta kratší období pokrývající aktuální období.

Kategorie aktivit

Detekované aktivity jsou pro přehlednost řazeny do několika kategorií. Pod názvem každé kategorie jsou uvedeny sumární informace (celkový počet spojení, celkový objem přenesených dat apod.) a dále následují podrobnosti o jednotlivých aktivitách. Podrobnosti lze volitelně skrýt. Je-li zvoleno období delší než jeden den, pak jsou navíc záznamy v každé kategorii rozděleny po jednotlivých dnech. Denní záznamy lze rovněž volitelně skrýt.

U každého záznamu o aktivitě jsou uvedeny dva časové údaje: čas zahájení aktivity a délka (doba trvání) aktivity. Je-li aktivita označena jako nedokončená, znamená to, že je příslušné spojení stále otevřené.

Kategorie aktivit se zobrazují vždy v pořadí, jak jsou uvedeny v následujícím popisu. Pokud uživatel neměl v daném období žádnou aktivitu patřící do určité kategorie, pak tato kategorie nebude zobrazena.

WWW stránky

Tato kategorie zahrnuje jednu z nejčastějších aktivit uživatelů — prohlížení WWW stránek a vyhledávání na Internetu.

Začátek	Délka	Podrobnosti
15:32	11:43	google.cz Návštěvy: 3 Google
15:32	0:01	google.cz: kerio
15:32	6:28	kerio.com Návštěvy: 1 Kategorie: Informační technologie Kerio Technologies Kerio VPN Client download
15:33	6:28	idnes.cz Návštěvy: 22 Kategorie: Informace / Komunikace IDNES.cz - nejdůvěryhodnější zpravodajský portál na českém internetu
15:34	2:25	billboard.cz Návštěvy: 4 TakeIt.cz
15:40	1:57	radiotv.cz Návštěvy: 5 Kategorie: Zábava / Kultura Rádía a televize - co se děje v éteru - Czech Radio and TV [RadioTV.cz]
15:43		google.cz: edonkey
15:43		google.cz: edonkey download
15:44	4:30	wikipedia.org Návštěvy: 3 Kategorie: Společnost / Vzdělání / Náboženství, Informace / Komunikace eDonkey network - Wikipedia, the free encyclopedia
15:48	0:01	emule-project.net Návštěvy: 1 Kategorie: Informační technologie eMule-Project.net - Official eMule Homepage. Downloads, Help, Docu, News...
15:48	0:12	sourceforge.net Návštěvy: 2 Kategorie: Informační technologie SourceForge.net: Downloading ...

Obrázek 3.14 Aktivita uživatele — přístup na WWW stránky

V záhlaví je uveden celkový počet navštívených WWW stránek v daném období a celkový počet vyhledávání na Internetu. *WinRoute* dokáže správně detekovat většinu běžných internetových vyhledávačů.

Záznam o přístupu na WWW stránku obsahuje:

- Čas zahájení a délku aktivity (viz výše).
- Doménu, do které stránka patří (statistiky v rozhraní *StaR* se vytvářejí podle domén — viz např. kapitola 3.7).
- Počet návštěv stránky — kolikrát byla stránka navštívena v rámci této aktivity.
- Kategorie stránky — klasifikace stránky modulem *Kerio Web Filter*. Pokud není modul *Kerio Web Filter* aktivní nebo se stránku nepodařilo klasifikovat, kategorie stránky nebude zobrazena.

- Titulek stránky. Titulek je zobrazen jako odkaz — po kliknutí na titulek se příslušná stránka otevře v novém okně prohlížeče (resp. nové záložce). Pokud stránka nemá titulek, nebude v přehledu aktivit uživatele zobrazena.

Při přístupu na zabezpečené (*HTTPS*) stránky je komunikace šifrována, a proto nelze zjistit titulky ani URL jednotlivých stránek. V záznamu jsou pak uvedeny pouze tyto údaje:

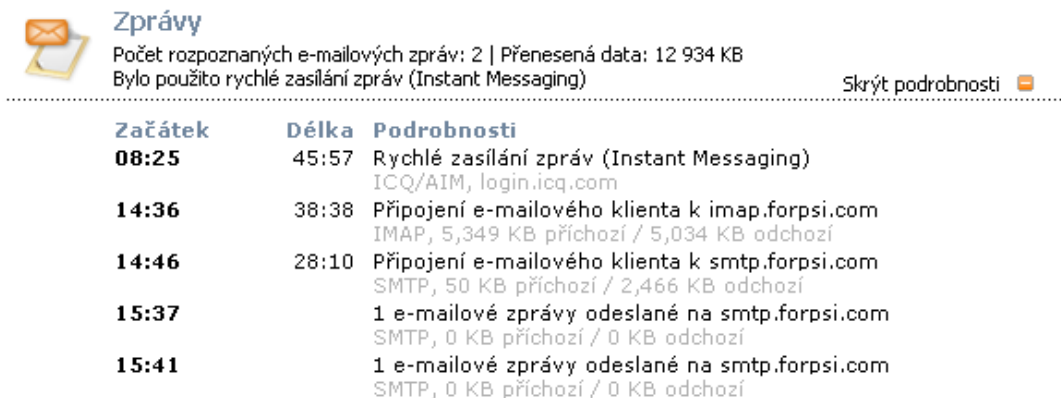
- Jméno (případně IP adresa) serveru.
- Protokol (*HTTPS*).
- Objem přenesených dat v každém směru.

Záznam o vyhledávání obsahuje:

- Vyhledávač (pouze doménu).
- Hledaný výraz. Výraz je zobrazen jako odkaz, kliknutím bude vyhledán v příslušném vyhledávači a výsledek zobrazen v novém okně prohlížeče (resp. nové záložce).

Zprávy (e-mail a rychlé zasílání zpráv)

Tato kategorie zahrnuje dva typy aktivit: e-mailovou komunikaci (protokoly *SMTP*, *IMAP* a *POP3*) a rychlé zasílání zpráv (*Instant Messaging* — služby *ICQ*, *AOL Instant Messenger* (*AIM*), *Yahoo! Messenger*, *MSN Messenger* apod.).



Začátek	Délka	Podrobnosti
08:25	45:57	Rychlé zasílání zpráv (Instant Messaging) ICQ/AIM, login.icq.com
14:36	38:38	Připojení e-mailového klienta k imap.forpsi.com IMAP, 5,349 KB příchozí / 5,034 KB odchozí
14:46	28:10	Připojení e-mailového klienta k smtp.forpsi.com SMTP, 50 KB příchozí / 2,466 KB odchozí
15:37		1 e-mailové zprávy odeslané na smtp.forpsi.com SMTP, 0 KB příchozí / 0 KB odchozí
15:41		1 e-mailové zprávy odeslané na smtp.forpsi.com SMTP, 0 KB příchozí / 0 KB odchozí

Obrázek 3.15 Aktivita uživatele — e-mail a rychlé zasílání zpráv

V hlavičce je uveden počet detekovaných e-mailových zpráv a celkový objem dat přenesených e-mailovými protokoly. E-mailové zprávy *WinRoute* rozpoznává pouze v protokolech *SMTP* a *POP3*, pokud komunikace není šifrována. V ostatních případech (protokol *IMAP*, šifrovaná komunikace atd.) je sledován pouze objem dat přenesených jednotlivými protokoly.

V kategorii *Zprávy* se zobrazují tyto typy záznamů:

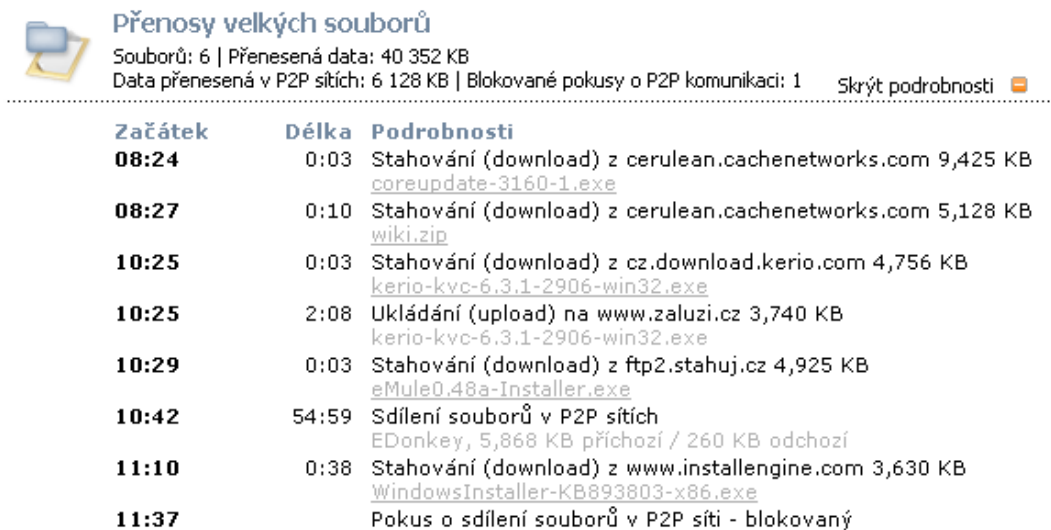
- Připojení k serveru — připojení poštovního klienta k *SMTP*, *IMAP* nebo *POP3* serveru. V záznamu je uvedeno jméno (případně IP adresa) příslušného serveru, použitý protokol a objem přenesených dat v každém směru.
- Odeslané/přijaté zprávy — počet zpráv (přenesených v rámci jednoho připojení), jméno (případně IP adresa) serveru odchozí/příchozí pošty, použitý protokol a objem přenesených dat v každém směru.

Poznámka: Objem přenesených dat je zaokrouhlován na celé kilobyty. Je-li objem dat menší než 0.5 KB, zobrazí se hodnota 0.

- Rychlé zaslání zpráv — zaznamenává se pouze přihlášení uživatele k serveru. V záznamu je uveden protokol (služba rychlého zaslání zpráv) a jméno (případně IP adresa) přihlašovacího serveru. Délka aktivity v tomto případě znamená pouze dobu, po kterou byl uživatel přihlášen k příslušné službě, bez ohledu na to, zda posílal zprávy či nikoliv.

Přenosy velkých souborů

Tato kategorie zahrnuje uživatelské aktivity, při kterých se přenášejí velké objemy dat — typicky stahování (download) souborů z WWW a FTP serverů, ukládání (upload) souboru na FTP server nebo sdílení souborů v P2P sítích. Za „velký soubor“ je považován soubor o velikosti větší než 1 MB (případně 2 MB dat přenesených neznámým spojením — viz dále).



Začátek	Délka	Podrobnosti
08:24	0:03	Stahování (download) z cerulean.cachenetworks.com 9,425 KB coreupdate-3160-1.exe
08:27	0:10	Stahování (download) z cerulean.cachenetworks.com 5,128 KB wiki.zip
10:25	0:03	Stahování (download) z cz.download.kerio.com 4,756 KB kerio-kvc-6.3.1-2906-win32.exe
10:25	2:08	Ukládání (upload) na www.zaluzi.cz 3,740 KB kerio-kvc-6.3.1-2906-win32.exe
10:29	0:03	Stahování (download) z ftp2.stahuj.cz 4,925 KB eMule0.48a-Installer.exe
10:42	54:59	Sdílení souborů v P2P sítích EDonkey, 5,868 KB přichází / 260 KB odchozí
11:10	0:38	Stahování (download) z www.installengine.com 3,630 KB WindowsInstaller-KB893803-x86.exe
11:37		Pokus o sdílení souborů v P2P síti - blokováný

Obrázek 3.16 Aktivita uživatele — přenosy velkých souborů a používání P2P sítí

V hlavičce je uveden celkový počet rozpoznaných souborů, celkový objem přenesených dat (v obou směrech), objem dat přenesených v P2P sítích (rovněž v obou směrech) a počet blokováných pokusů o sdílení souborů v P2P sítích (tento údaj se zobrazuje, pouze byl-li nějaký pokus detekován a blokován).

Typy záznamů v kategorii *Přenosy velkých souborů*:

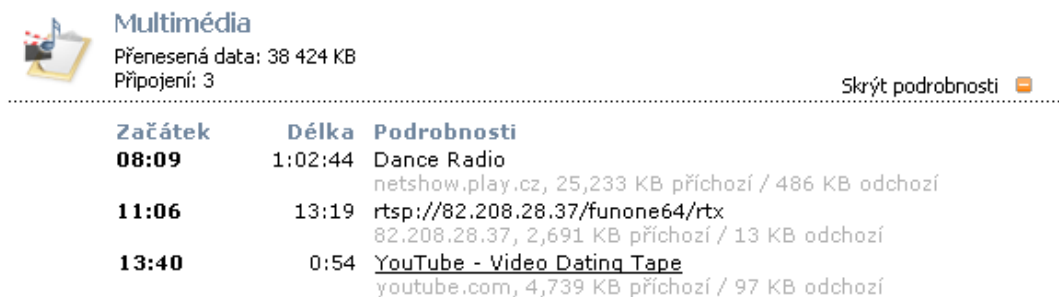
- Stahování (download) nebo ukládání (upload) souboru — záznam obsahuje jméno (případně IP adresu) serveru, objem přenesených dat a název přenášeného souboru. Jedná-li se o stahování souboru z WWW serveru nebo anonymního FTP serveru, pak je název souboru zobrazen jako odkaz. Kliknutím na odkaz lze tento soubor stáhnout ze serveru tak, jak jej stahoval příslušný uživatel.
- Sdílení (přenosy) souborů v P2P sítích — záznam obsahuje jméno detekované P2P sítě a objem přenesených dat v každém směru.
- Blokováný pokus o použití P2P sítě — informace o tom, že se uživatel pokusil sdílet soubory v P2P síti, ale jeho pokus byl detekován a zablokován modulem

P2P Eliminator.

- Neznámé spojení — libovolná komunikace daného uživatele mezi lokální sítí a Internetem, při které bylo přeneseno více než 2 MB dat a zároveň nepatří do jiné kategorie (např. *Multimédia*). Záznam obsahuje jméno nebo IP adresu serveru, protokol/službu (pokud byla rozpoznána) a objem přenesených dat v každém směru.

Multimédia

Kategorie *Multimédia* zahrnuje přenos multimediálních dat v reálném čase — tzv. *streaming* (typicky internetová rádia a televize).



Začátek	Délka	Podrobnosti
08:09	1:02:44	Dance Radio netshow.play.cz, 25,233 KB příchozí / 486 KB odchozí
11:06	13:19	rtsp://82.208.28.37/funone64/rtx 82.208.28.37, 2,691 KB příchozí / 13 KB odchozí
13:40	0:54	<u>YouTube - Video Dating Tape</u> youtube.com, 4,739 KB příchozí / 97 KB odchozí

Obrázek 3.17 Aktivita uživatele — multimédia

V hlavičce je uveden celkový objem dat přenesený multimediálními protokoly a celkový počet připojení k serverům.

Záznamy o jednotlivých aktivitách obsahují tyto informace:

- Název streamu (případně URL, není-li název k dispozici). Za určitých podmínek může být název zobrazen jako odkaz, kterým lze příslušný stream přímo otevřít.
- Jméno (případně IP adresu) serveru.
- Objem přenesených dat v každém směru.

Vzdálený přístup

Tato kategorie zahrnuje jednak vzdálený přístup uživatele na počítače v Internetu (např. *Microsoft Remote Desktop (RDP — Vzdálená plocha)*, *VNC*, ale také *Telnet* a *SSH*) a jednak přístup do vzdálených sítí prostřednictvím VPN. Vzdálený přístup, pokud neslouží k pracovním účelům, je poměrně nebezpečná aktivita. Uživatel takto může snadno obejít pravidla firewallu ve své lokální síti — např. prohlížením zakázaných WWW stránek na vzdáleném počítači nebo přenášením nepovolených souborů pomocí VPN.



Začátek	Délka	Podrobnosti
07:59	1:12:05	doma.novak.cz RDP, 3,716 KB příchozí / 90,303 KB odchozí
10:23	1:14:20	doma.novak.cz RDP, 1,135 KB příchozí / 19,777 KB odchozí
14:06	20:12	vpn.server.cz Kerio VPN, 4,458 KB příchozí / 256 KB odchozí

Obrázek 3.18 Aktivita uživatele — vzdálený přístup a používání VPN

Hlavička kategorie *Vzdálený přístup* obsahuje:

- počet VPN připojení a celkový objem dat přenesených prostřednictvím VPN,
- počet vzdálených přístupů a celkový objem přenesených dat.

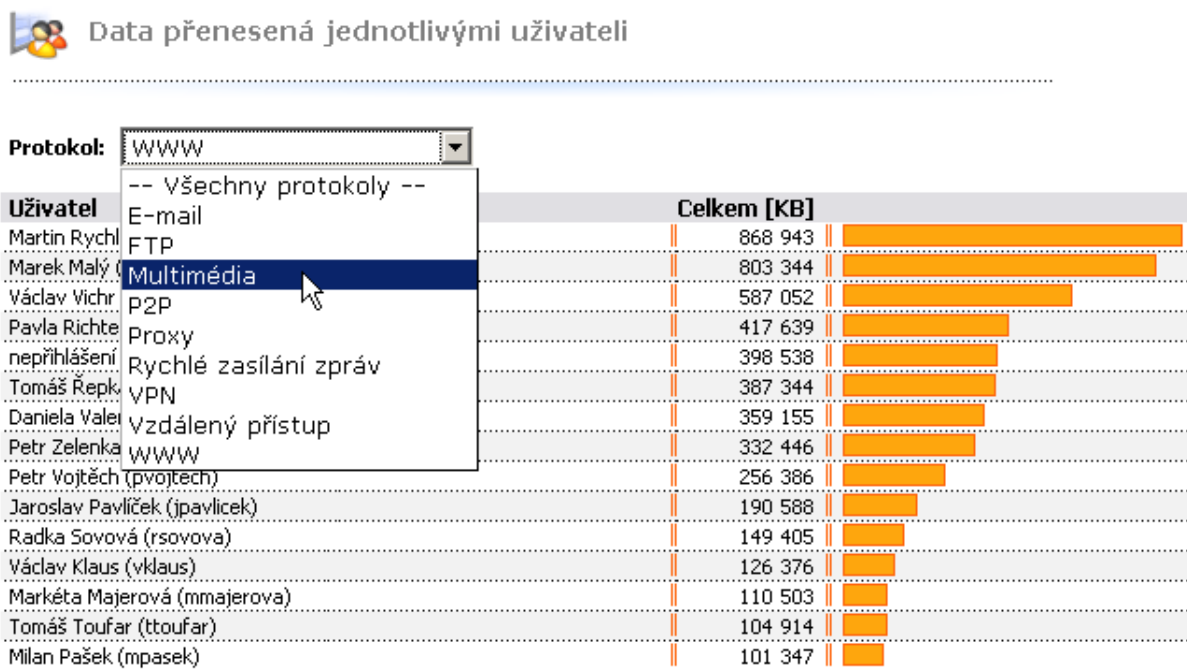
Záznamy o jednotlivých aktivitách obsahují tyto informace:

- jméno (případně IP adresu) serveru, ke kterému se uživatel připojuje,
- název protokolu/služby,
- objem dat přenesených daným připojením v každém směru.

3.6 Přehled uživatelů podle objemu přenesených dat

Sekce *Komunikace uživatelů* zobrazuje tabulku všech uživatelů seřazenou sestupně podle objemu přenesených dat. Tato tabulka dává přehled o tom, jak se který uživatel podílel na celkovém objemu přenesených dat. V tabulce lze zobrazit veškerá přenesená data, nebo pouze data přenesená vybraným protokolem (resp. třídou protokolů). Takto lze získat přehled o tom, kteří uživatelé přenesli nejvíce dat určitou službou (např. poslechem internetových rádií).

Poznámka: Podrobný popis tříd protokolů rozlišovaných v rozhraní *Kerio Star* viz kapitola [3.3](#).



Obrázek 3.19 Tabulka uživatelů podle objemu přenesených dat

Každý řádek tabulky obsahuje jméno uživatele a objem dat přenesených tímto uživatelem: příchozí data (download), odchozí data (upload) a celkový objem dat. Je-li vybrán konkrétní protokol, zobrazuje se pouze celkový objem přenesených dat.

Kliknutím na jméno vybraného uživatele se stránka přepne na záložku *Uživatelé* a zobrazí se podrobné statistiky vybraného uživatele (viz kapitola [3.4](#)).

Tip

Způsob zobrazení uživatelského jména v tabulce lze nastavit v konfiguraci *WinRoute*.

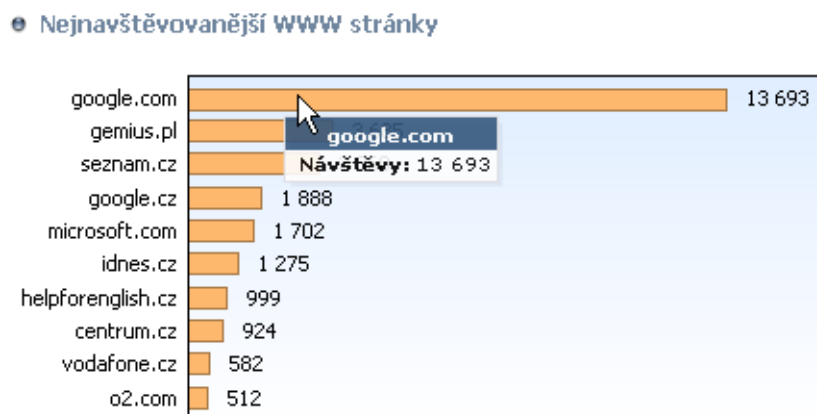
3.7 Nejnavštěvovanější WWW stránky

Záložka *WWW stránky* obsahuje statistiky deseti nejnavštěvovanějších WWW domén. Z těchto statistik lze zjistit např.:

- které stránky (domény) uživatelé pravidelně navštěvují,
- kteří uživatelé jsou neaktivnější v „brouzdání“ po webových stránkách.

Graf v horní části záložky zobrazuje deset nejnavštěvovanějších WWW domén. Číselný údaj v grafu znamená počet návštěv všech WWW stránek z příslušné domény v daném reportovacím období.

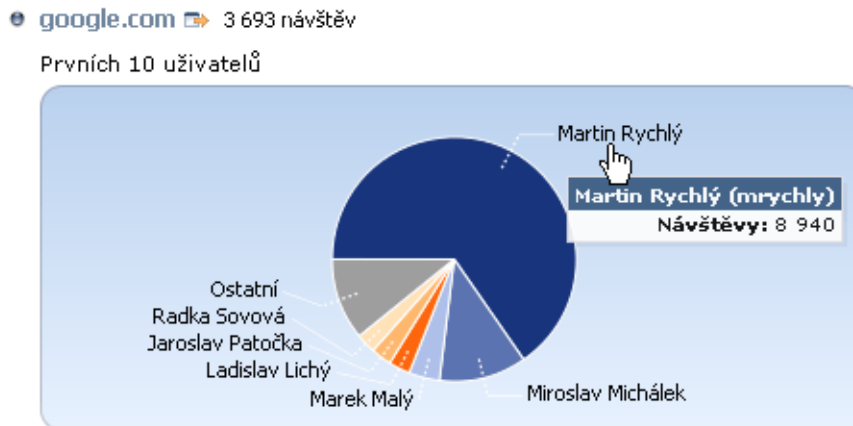
Poznámka: *WinRoute* „vidí“ pouze jednotlivé HTTP požadavky. Pro zjištění počtu návštěv stránek (tj. vyhodnocení, které požadavky byly vyslány v rámci jedné návštěvy) se používá speciální heuristický algoritmus. Z tohoto důvodu nejsou údaje o počtu návštěv absolutně přesné, jedná se však o velmi dobrou aproximaci.



Obrázek 3.20 Nejnavštěvovanější WWW domény

Pod grafem jsou zobrazeny podrobné statistiky pro každou z deseti nejnavštěvovanějších domén:

- V záhlaví je vždy uveden název DNS domény a celkový počet návštěv WWW stránek na serverech v této doméně. Název domény je zároveň odkaz na „výchozí“ WWW stránku v dané doméně (před název domény se připojí jméno *www*, tedy např. pro doménu *google.com* se otevře stránka *www.google.com*).
- Koláčový graf zobrazuje podíl (nejvýše šesti) neaktivnějších uživatelů na celkové návštěvnosti dané domény. Při umístění kurzoru myši na jméno vybraného uživatele se zobrazí celkový počet WWW stránek navštívených tímto uživatelem.



Obrázek 3.21 Graf nejaktivnějších uživatelů pro danou doménu

- Tabulka vedle grafu obsahuje nejaktivnější uživatele seřazené podle počtu návštěv WWW stránek v dané doméně (nejvýše deset uživatelů).

Uživatel	Návštěvy
Martin Rychlý (mrychly)	8 940
Miroslav Michálek (mmichalek)	1 588
Marek Malý (mmaly)	560
Ladislav Lichý (lichy)	391
Jaroslav Patočka (jpatocka)	375
Radka Sovová (rsovova)	357
Karel Lukeš (klukes)	294
Petr Zelenka (pzelenka)	222
Petr Vojtěch (pvojtech)	144
Václav Klaus (vklaus)	98

Obrázek 3.22 Tabulka nejaktivnějších uživatelů pro danou doménu

Kliknutím na jméno vybraného uživatele v tabulce nebo v grafu se stránka přepne na záložku *Uživatelé* a zobrazí se podrobné statistiky vybraného uživatele (viz kapitola 3.4).

Tip

Způsob zobrazení uživatelského jména v tabulce lze nastavit v konfiguraci *WinRoute*. V grafu je vždy zobrazováno pouze celé jméno uživatele (případně uživatelské jméno, pokud není celé jméno v uživatelském účtu vyplněno).

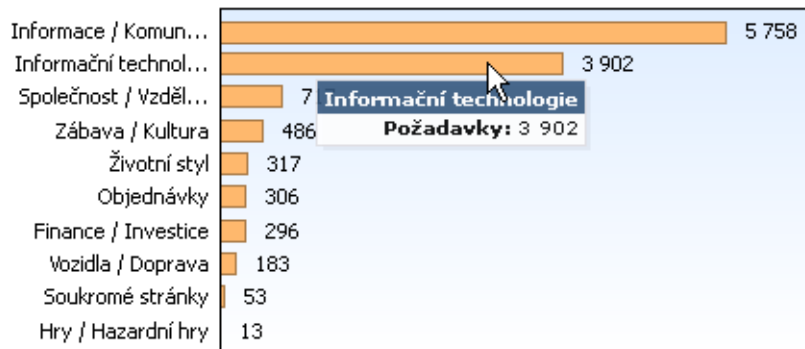
3.8 Nejnavštěvovanější kategorie WWW stránek

Záložka *WWW stránky* obsahuje statistiky deseti nejnavštěvovanějších kategorií WWW stránek dle kategorizace modulem *Kerio Web Filter*. Statistiky kategorií dávají obecnější přehled o navštívených WWW stránkách. Tyto statistiky poskytují např. informaci o tom, v jaké míře uživatelé navštěvují WWW stránky nepracovního charakteru.

Graf v levé části záložky zobrazuje deset nejnavštěvovanějších kategorií WWW stránek v daném reportovacím období. Číselný údaj v grafu znamená absolutní počet HTTP požadavků

zařazených do dané kategorie. Technicky není možné rozlišit, zda se jedná o požadavky při načítání jedné stránky nebo požadavky na různé stránky. Z tohoto důvodu jsou počty požadavků zpravidla výrazně vyšší než počty návštěv ve statistikách nejnavštěvovanějších WWW stránek (viz kapitola 3.7).

• Nejnavštěvovanější kategorie stránek



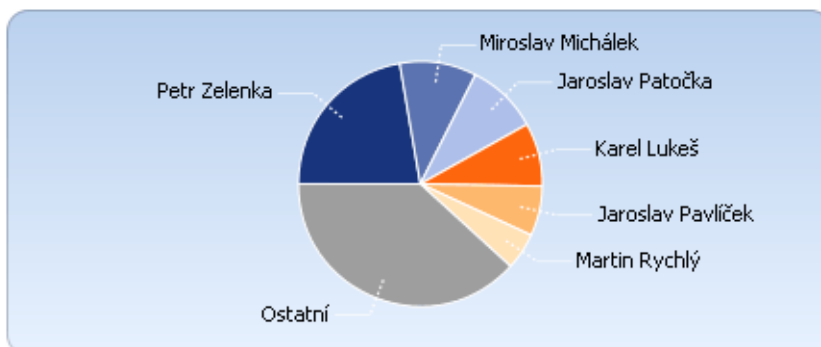
Obrázek 3.23 Nejnavštěvovanější kategorie WWW stránek dle počtu požadavků

Pod grafem jsou k dispozici podrobné statistiky pro každou z deseti nejnavštěvovanějších kategorií WWW stránek:

- V záhlaví je vždy uveden název kategorie a celkový počet požadavků na WWW stránky z této kategorie.
- Koláčový graf zobrazuje podíl (nejvýše šesti) nejaktivnějších uživatelů na celkové návštěvnosti stránek dané kategorie. Při umístění kurzoru myši na jméno vybraného uživatele se zobrazí celkový počet požadavků tohoto uživatele na danou kategorii WWW stránek.

• Informace / Komunikace 5 758 požadavků

Prvních 10 uživatelů



Obrázek 3.24 Graf nejaktivnějších uživatelů pro danou kategorii WWW stránek

- Tabulka vedle grafu obsahuje neaktivnější uživatele seřazené podle počtu požadavků na danou kategorii stránek (nejvýše deset uživatelů).

Uživatel	Požadavky
Petr Zelenka (pzelenka)	1 284
Miroslav Michálek (mmichalek)	586
Jaroslav Patočka (jpatocka)	544
Karel Lukeš (klukes)	483
Jaroslav Pavlíček (jpavlicek)	379
Martin Rychlý (mrychly)	281
Zdeněk Ruml (zruml)	247
Milan Pašek (mpasek)	206
Radka Sovová (rsovova)	195
Václav Suda (vsuda)	182

Obrázek 3.25 Tabulka neaktivnějších uživatelů pro danou kategorii WWW stránek

Kliknutím na jméno vybraného uživatele v tabulce nebo v grafu se stránka přepne na záložku *Uživatelé* a zobrazí se podrobné statistiky vybraného uživatele (viz kapitola [3.4](#)).

Tip

Způsob zobrazení uživatelského jména v tabulce lze nastavit v konfiguraci *WinRoute*. V grafu je vždy zobrazováno pouze celé jméno uživatele (případně uživatelské jméno, pokud není celé jméno v uživatelském účtu vyplněno).

Poznámka: Statistiky kategorií navštívených stránek mohou být ovlivněny úspěšností kategorizace jednotlivých stránek. Některé stránky mohou být z technických důvodů nekategorizované nebo (výjimečně) zařazené do nesprávné kategorie.

Kapitola 4

Kerio Clientless SSL-VPN

Kerio Clientless SSL-VPN (dále jen „*SSL-VPN*“) je speciální rozhraní umožňující zabezpečený vzdálený přístup prostřednictvím WWW prohlížeče ke sdíleným prostředkům (souborům a složkám) v síti, kterou *WinRoute* chrání.

Rozhraní *SSL-VPN* je do jisté míry alternativou k aplikaci *Kerio VPN Client*. 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*.

4.1 Použití rozhraní SSL-VPN

Pro přístup k rozhraní lze využít většinu běžných grafických WWW prohlížečů (viz kapitola 1). Do prohlížeče zadáme URL ve tvaru

`https://server/`

kde *server* je jméno nebo IP adresa počítače s *WinRoute*. Používá-li *SSL-VPN* jiný port než standardní port služby *HTTPS* (443), pak je třeba v URL uvést také příslušný port — např.:

`https://server:12345/`

Po připojení k serveru se zobrazí přihlašovací stránka rozhraní *SSL-VPN* v jazyce dle nastavení prohlížeče. Není-li k dispozici lokalizace pro žádný z jazyků preferovaných v prohlížeči, bude použita angličtina.

Pro přístup do sítě prostřednictvím *SSL-VPN* je nutné se ověřit zadáním uživatelského jména a hesla do příslušné domény na přihlašovací stránce. Přihlašovací údaje jsou ve většině případů shodné jako pro přihlášení do systému na počítači uživatele. Veškeré operace se sdílenými soubory a složkami budou prováděny pod identitou přihlášeného uživatele.



Kerio Clientless SSL-VPN

Přihlášení do Kerio Clientless SSL-VPN:

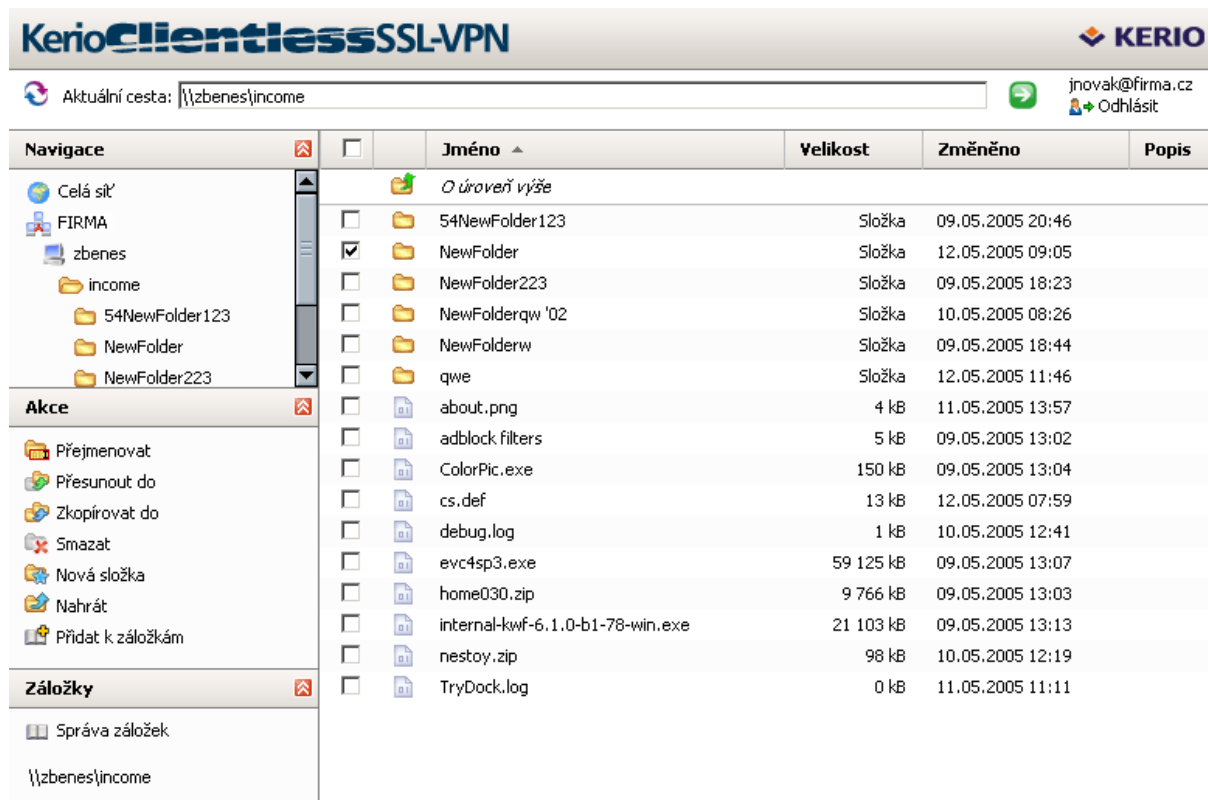
Jméno:

Heslo:

Obrázek 4.1 Clientless SSL-VPN — přihlašovací dialog

Práce se soubory a složkami

Práce s rozhraním *SSL-VPN* je velmi podobná práci se systémovým oknem *Místa v síti* (*My Network Places*).



Obrázek 4.2 Clientless SSL-VPN — hlavní stránka

V horní části stránky je k dispozici adresní řádek, do kterého lze přímo zadat umístění požadovaného sdíleného prostředku (tzv. *UNC cestu*) — např.:

```
\\server\složka\podslózka
```

Cestu lze zapsat normálním způsobem, i když názvy složek a/nebo souborů obsahují mezery — např.:

```
\\server\moje složka\můj soubor.doc
```

Všechny sdílené prostředky v doméně lze procházet pomocí tzv. navigačního stromu v levé části stránky. Navigační strom je provázán s adresním řádkem (tzn. v adresním řádku se vždy zobrazuje cesta k položce vybrané ve stromu a naopak při zadání cesty do adresního řádku se ve stromu zobrazí odpovídající položka).

Pod navigačním stromem je zobrazen seznam akcí, které lze provést v daném umístění (resp. pro vybraný soubor nebo složku). Základními funkcemi, které rozhraní *SSL-VPN* nabízí, je stažení vybraného souboru na lokální počítač (tzn. počítač, na kterém je spuštěn WWW prohlížeč uživatele) a nahrání souboru z lokálního počítače do vybraného umístění ve vzdálené doméně

(uživatel musí mít právo zápisu do cílového umístění). Stažení nebo nahrání více souborů zároveň nebo celých složek není možné.

Pro soubory a složky jsou dále k dispozici všechny standardní funkce — kopírování, přejmenování, přesun, mazání. Kopírovat nebo přesunovat soubory a složky je možné v rámci sdílených prostředků v dané doméně. V aktuálním umístění lze vytvářet nové složky a mazat prázdné složky.

Antivirová kontrola

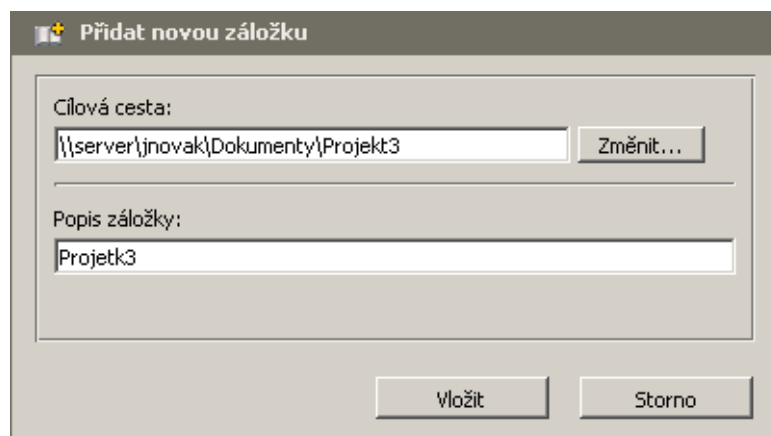
Správce *WinRoute* může nastavit antivirovou kontrolu souborů přenášených rozhraním *SSL-VPN* (standardně se provádí kontrola ukládaných souborů). Rozhraní *SSL-VPN* tak zaručuje bezpečnost při přenášení souborů mezi klientským počítačem a vzdálenou lokální sítí. Pokud je ve stahovaném nebo ukládaném souboru nalezen virus, operace bude přerušena a zobrazí se varování.

Záložky

Pro rychlý přístup k často používaným síťovým prostředkům si uživatel může vytvořit tzv. záložky. Záložky jsou obdobou *Oblíbených položek (Favorites)* v systému *Windows*.

Volbou *Přidat k záložkám* lze vytvořit záložku pro aktuální umístění (tj. pro cestu zobrazenou v adresním řádku). Záložku doporučujeme pojmenovat krátkým výstižným názvem — dobré pojmenování usnadňuje orientaci zejména při větším počtu záložek. Pokud nebude název záložky vyplněn, bude v seznamu záložek zobrazována přímo odpovídající UNC cesta.

Volba *Správa záložek* umožňuje upravit nebo smazat již vytvořené záložky, případně vytvořit novou záložku pro libovolnou cílovou cestu (složku). Cílovou složku lze zadat ručně nebo ji vyhledat ve stromu složek, případně je možné použít jako výchozí bod jinou již existující záložku.



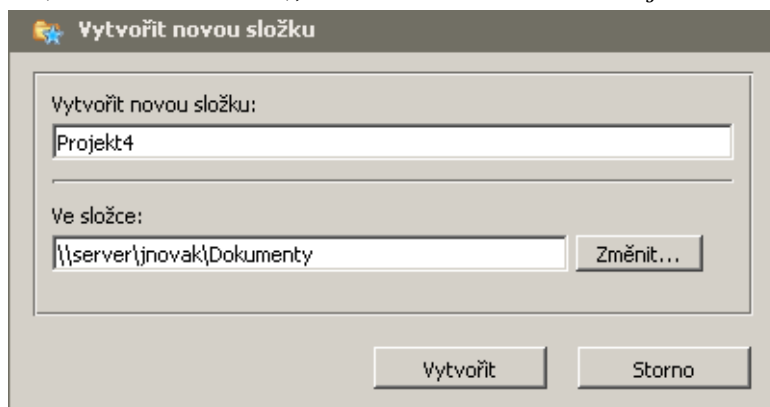
Obrázek 4.3 Clientless SSL-VPN — vytvoření záložky

Příklady operací se soubory a složkami

V této sekci uvádíme několik praktických ukázek práce se soubory a složkami prostřednictvím rozhraní SSL-VPN.

Vytvoření nové složky

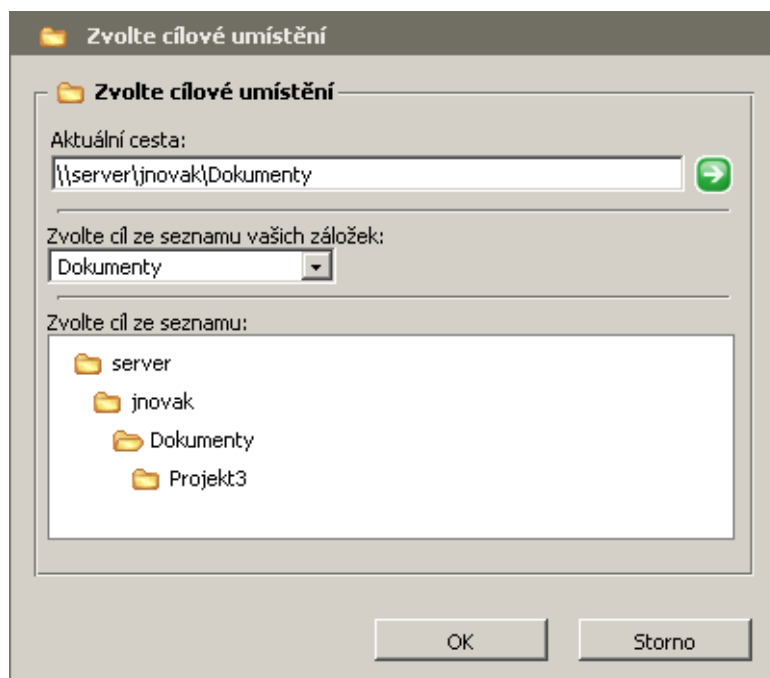
Dialog umožňuje vytvořit novou složku ve zvoleném umístění. Standardně je nabízena aktuální cesta (z adresního řádku), lze však zadat libovolnou jinou cestu.



Obrázek 4.4 Clientless SSL-VPN — vytvoření nové složky

Tlačítko *Změnit* nabízí další možnosti výběru cesty (složky), ve které má být nová složka vytvořena:

- použití záložky,
- výběr ze stromu složek.



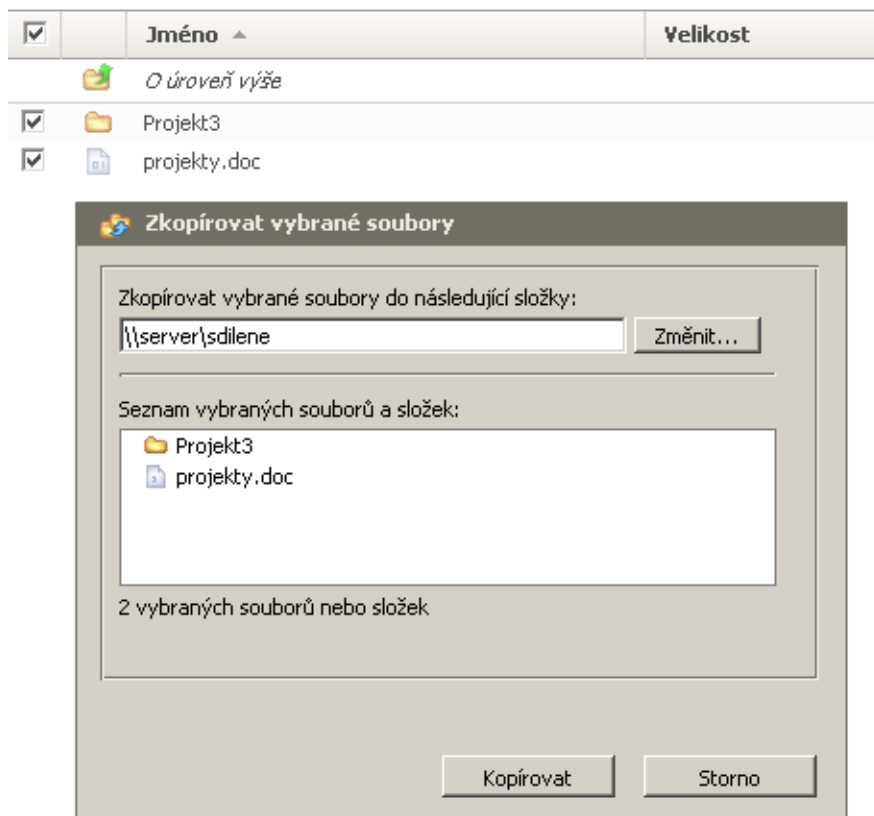
Obrázek 4.5 Clientless SSL-VPN — výběr cílové cesty (složky)

Přejmenování souboru nebo složky

Přejmenování je triviální operace — dialog umožňuje pouze zadat nové jméno pro vybraný soubor nebo složku.

Kopírování nebo přesun souborů / složek

Rozhraní *SSL-VPN* umožňuje kopírovat nebo přesunovat libovolný počet souborů a složek současně. Požadované soubory a složky nejprve označíme pomocí zaškrtnutých polí vedle názvu (zaškrtnutím pole v záhlaví lze označit všechny soubory a složky v aktuální cestě).



Obrázek 4.6 Clientless SSL-VPN — kopírování nebo přesun souborů / složek

V dialogu pro kopírování nebo přesun pak zadáme cílovou cestu (složku), případně ji vybereme ze stromu nebo použijeme záložku (viz výše).

Mazání souborů / složek

Podobně jako v případě kopírování nebo přesunu lze současně smazat libovolný počet souborů a složek, případně všechny soubory a složky v aktuální cestě.

Stažení (download) souboru

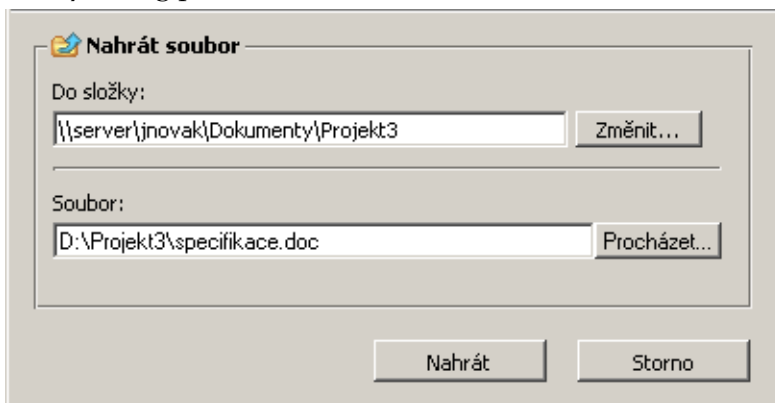
Stažení souboru ze sdílené složky ve vzdálené síti na lokální počítač probíhá stejným způsobem jako stažení jakéhokoliv souboru z WWW stránek. Po kliknutí na vybraný soubor se otevře standardní systémový dialog pro uložení souboru.

Stažení více souborů nebo celých složek najednou není možné.

Nahrání (upload) souboru

Dialog pro nahrání souboru umožňuje výběr cílové složky (standardně je nabízena složka aktuálně otevřená v rozhraní *SSL-VPN*). Cílovou složku je možné zadat ručně, vybrat ze stromu nebo použít vytvořenou záložku (viz výše).

Do pole *Soubor* je třeba zadat kompletní cestu k požadovanému souboru na lokálním disku. Soubor je rovněž možné vyhledat tlačítkem *Procházet...* (toto tlačítko zobrazí standardní systémový dialog pro otevření souboru).



Obrázek 4.7 Clientless SSL-VPN — nahrání souboru do sdílené složky

Nahrání více souborů nebo celých složek najednou není možné.

Příloha A

Právní doložka

Microsoft®, *Windows®*, *Windows NT®*, *Windows Vista™*, *Internet Explorer®*, *ActiveX®*, a *Active Directory®* jsou registrované ochranné známky nebo ochranné známky společnosti *Microsoft Corporation*.

Mac OS® a *Safari™* jsou registrované ochranné známky nebo ochranné známky společnosti *Apple Computer, Inc.*

Linux® je registrovaná ochranná známka, jejímž držitelem je Linus Torvalds.

Mozilla® a *Firefox®* jsou registrované ochranné známky společnosti *Mozilla Foundation*.

Kerberos™ je ochranná známka *Massachusetts Institute of Technology (MIT)*.

Ostatní uvedené názvy skutečných společností a produktů mohou být registrovanými ochrannými známkami nebo ochrannými známkami jejich vlastníků.

Slovníček pojmů

ActiveX

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

Technologie *ActiveX* je podporována pouze ve WWW prohlížeči *Internet Explorer* v operačním systému *Microsoft Windows*.

Firewall

Software nebo hardwarové zařízení, které chrání počítač nebo počítačovou síť před průnikem zvenčí (typicky z Internetu).

Pro účely tohoto manuálu je výrazem *firewall* označován počítač, na kterém je nainstalován *WinRoute*.

FTP

Protokol pro přenos souborů (*File Transfer Protocol*).

IMAP

Internet Message Access Protocol je protokol elektronické pošty umožňující klientům pracovat se svými zprávami na serveru bez nutnosti stahování na lokální počítač. Uživatel se tak může připojovat k serveru z více různých počítačů a má vždy k dispozici všechny své zprávy.

IP adresa

32-bitové číslo jednoznačně určující počítač v Internetu. Zapisuje v desítkové soustavě jako čtveřice bytů (0–255) oddělených tečkami (např. 195 . 129 . 33 . 1).

P2P síť

Peer-to-Peer síť (zkr. *P2P* síť) 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*.

POP3

Post Office Protocol je protokol pro přístup k elektronické poště, který umožňuje uživatelům stahovat zprávy ze serveru na lokální disk. Je vhodný zejména pro klienty, kteří nemají trvalé připojení k Internetu.

Port

16-bitové číslo (1–65535) používané protokoly TCP a UDP pro identifikaci aplikací (služeb) na daném počítači. Na jednom počítači (jedné IP adrese) může běžet více aplikací současně (např. WWW server, poštovní klient, WWW klient — prohlížeč, FTP klient atd.). Každá aplikace je však jednoznačně určena číslem portu. Porty 1–1023 jsou vyhrazené a používají je standardní, příp. systémové služby (např. 80 = WWW). Porty nad 1024 (včetně) mohou být volně použity libovolnou aplikací (typicky klientem jako zdrojový port nebo nestandardní aplikací serverového typu).

PPTP

Proprietární protokol firmy *Microsoft* pro vytváření virtuálních privátních sítí.

[Viz VPN.](#)

Proxy server

Starší, avšak stále poměrně rozšířený způsob sdílení internetového připojení. Proxy server představuje prostředníka mezi klientem a cílovým serverem.

Proxy server pracuje na aplikační úrovni a je přizpůsoben několika konkrétním aplikačním protokolům (např. HTTP, FTP, Gopher). Vyžaduje rovněž podporu v příslušné klientské aplikaci (např. WWW prohlížeči). Ve srovnání s technologií NAT jsou jeho možnosti velmi omezené.

Skript

Výkonný kód na WWW stránce, který provádí klient (WWW prohlížeč). Skripty slouží k vytváření dynamických prvků na WWW stránkách, mohou však být zneužity pro zobrazování reklam, získávání informací o uživateli apod. Moderní WWW prohlížeče podporují několik skriptovacích jazyků, mezi nejrozšířenější patří *JavaScript* a *Visual Basic Script (VBScript)*.

SMTP

Simple Mail Transfer Protocol je základní protokol, který se používá pro odesílání elektronické pošty v Internetu. Odesílatel a příjemce zprávy je určen e-mailovou adresou.

Spojení

Virtuální obousměrný komunikační kanál mezi dvěma počítači.

[Viz též TCP](#)

SSL

Protokol *Secure Socket Layer* slouží k zabezpečení a šifrování TCP spojení. Původně byl navržen pro zabezpečení přenosu WWW stránek protokolem HTTP, dnes je využíván téměř všemi standardními internetovými protokoly — SMTP, POP3, IMAP, LDAP atd.

Na začátku komunikace se nejprve asymetrickou šifrou provede výměna šifrovacího klíče, který je pak použit pro (symetrické) šifrování vlastních dat.

TCP

Transmission Control Protocol je protokol transportní úrovně, který zaručuje spolehlivé a sekvenční doručení dat. Je využíván většinou aplikačních protokolů, které vyžadují spolehlivé přenesení všech dat (např. *HTTP*, *FTP*, *SMTP*, *IMAP* atd.).

TCP/IP

Společné označení pro komunikační protokoly používané v Internetu (např. *IP*, *ICMP*, *TCP*, *UDP* atd.). *TCP/IP* není konkrétní protokol!

UDP

User Datagram Protokol je protokol transportní úrovně, který přenáší data v jednotlivých zprávách (tzv. datagramech). Nevytváří spojení, nezaručuje spolehlivé a sekvenční doručení dat a neumožňuje řízení toku dat a opravu chyb. Je vhodný pro přenos malého objemu dat (např. DNS dotazy) nebo v případech, kdy je rychlost důležitější než spolehlivost (např. přenos zvuku a videa v reálném čase).

VPN

Virtuální privátní síť (*Virtual Private Network*, *VPN*) představuje bezpečné propojení privátních sítí (např. jednotlivých poboček firmy) přes Internet. Spojení mezi oběma sítěmi (tzv. tunel) je šifrováno, což zabraňuje odposlechu přenášených dat. Pro vytváření VPN existují speciální protokoly, mezi nejrozšířenější patří standard *IPSec* a *PPTP* (*Point-to-Point Tunnelling Protocol*) firmy *Microsoft*.

WinRoute obsahuje proprietární implementaci VPN nazvanou *Kerio VPN*.

Rejstřík

C

- Clientless SSL-VPN [32](#)
 - antivirová kontrola [34](#)
 - použití [32](#)
 - záložky [34](#)

P

- preferovaný jazyk [11](#)

S

- SSL-VPN [32](#)
 - antivirová kontrola [34](#)
 - použití [32](#)
 - záložky [34](#)
- StaR [13](#)
 - aktivita uživatelů [21](#)
 - celkový přehled [17, 20](#)
 - nejnavštěvovanější WWW stránky [28](#)
 - nejnavštěvovanější kategorie WWW stránek [29](#)
 - objem přenesených dat [27](#)
 - reportovací období [15](#)
 - zobrazení [13](#)

statistiky

- aktivita uživatelů [21](#)
- celkový přehled [17, 20](#)
- Kerio StaR [13](#)
- nejnavštěvovanější WWW stránky [28](#)
- nejnavštěvovanější kategorie WWW stránek [29](#)
- objem přenesených dat [27](#)
- reportovací období [15](#)
- ve WWW rozhraní [13](#)
- zobrazení [13](#)

V

- VPN
 - Kerio Clientless SSL-VPN [32](#)

W

- WWW rozhraní [5](#)
 - ovládání vytáčených linek [12](#)
 - preferovaný jazyk [11](#)
 - přihlašovací stránka [5](#)
 - statistiky uživatele [8](#)
 - uživatelské předvolby [9](#)

