Kerio WinRoute Firewall 6

Konfigurace krok za krokem

Kerio Technologies s.r.o.

Tento manuál popisuje postup konfigurace lokální sítě s použitím produktu *Kerio WinRoute Firewall* ve verzi *6.6.0*. Změny vyhrazeny.

Aktuální verzi produktu a manuálu naleznete na WWW stránkách http://www.kerio.com/kwfdwn.

Obsah

Kapitola 1

Úvod

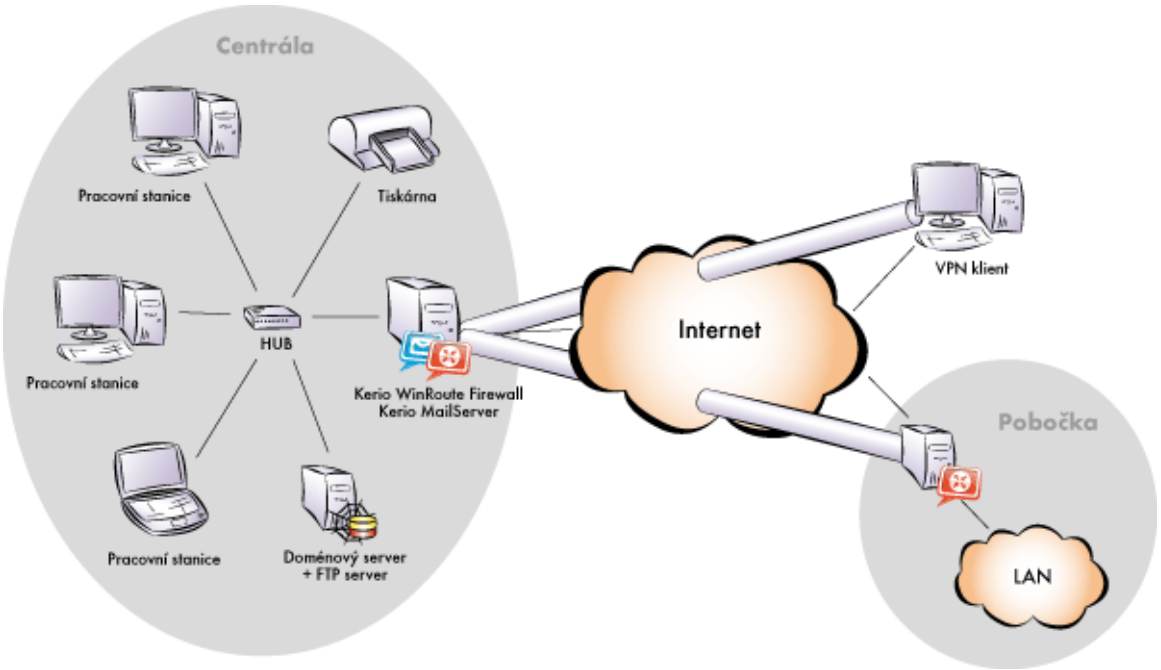
Tato příručka popisuje konfigurační úkony, které je třeba provést při nasazení aplikace *Kerio WinRoute Firewall* (dále jen *WinRoute*) v modelové síti. Uvažovaný model zohledňuje většinu požadavků, které vznikají při nasazení *WinRoute* v reálném prostředí — přístup z lokální sítě do Internetu, ochrana sítě proti průniku z Internetu, zpřístupnění vybraných služeb z Internetu, řízení přístupu uživatelů ke službám v Internetu, automatická konfigurace počítačů v lokální síti, ověřování uživatelů v *Active Directory* doméně atd.

Dalším požadavkem je propojení sítí v centrále a v pobočce firmy zabezpečeným šifrovaným kanálem (tzv. VPN tunel) a zabezpečený přístup klientů do lokální sítě přes Internet s využitím prostředků obsažených ve *WinRoute*.

Tato příručka je koncipována jako návod pro rychlé nastavení. Podrobnější informace k jednotlivým funkcím *WinRoute* a konfiguračním úkonům naleznete v manuálu *Kerio WinRoute Firewall — Příručka administrátora*, který je k dispozici na WWW stránce http://www.kerio.cz/kwf-manual/.

Modelová konfigurace sítě

Konfiguraci *WinRoute* popíšeme na modelovém příkladu sítě dle obrázku 1.1.



Obrázek 1.1 Modelová konfigurace sítě

Kapitola 2

Konfigurace sítě v centrále firmy

Tato kapitola obsahuje podrobný postup konfigurace lokální sítě a nastavení *WinRoute* v centrále firmy. Stejný postup lze použít i při konfiguraci sítě v pobočce firmy (pouze je třeba zvolit jinou IP subsíť).

Předpokládejme, že v lokální síti centrály firmy je vytvořena *Active Directory* doména `firma.cz` a všechny počítače v síti jsou členy této domény.

2.1 Volba IP adres pro lokální síť

V našem příkladu budeme uvažovat privátní sítě připojené do Internetu přes jednu veřejnou IP adresu. Celá lokální síť bude „skryta“ za touto IP adresou.

Pro lokální sítě, které nejsou součástí Internetu (tzv. privátní sítě), jsou vyhrazeny speciální rozsahy IP adres. Tyto adresy se nesmějí vyskytovat nikde v Internetu (internetové směrovače jsou zpravidla nastaveny tak, aby všechny pakety s těmito adresami zahazovaly).

Pro privátní sítě jsou vyhrazeny tyto rozsahy IP adres:

1. `10.x.x.x`, maska subsítě `255.0.0.0`
2. `172.16.x.x`, maska subsítě `255.240.0.0`
3. `192.168.x.x`, maska subsítě `255.255.0.0`

Upozornění

Použití jiných IP adres (mimo výše uvedené rozsahy) v privátní síti může mít za následek nedostupnost určitých částí Internetu (těch subsítí, které mají shodou okolností stejné IP adresy)!

Pro lokální síť centrály firmy zvolíme privátní IP adresy `192.168.1.x` s maskou subsítě `255.255.255.0` (IP subsíť `192.168.1.0`), pro síť pobočky IP adresy `10.1.1.x` s maskou `255.255.255.0` (IP subsíť `10.1.1.0`).

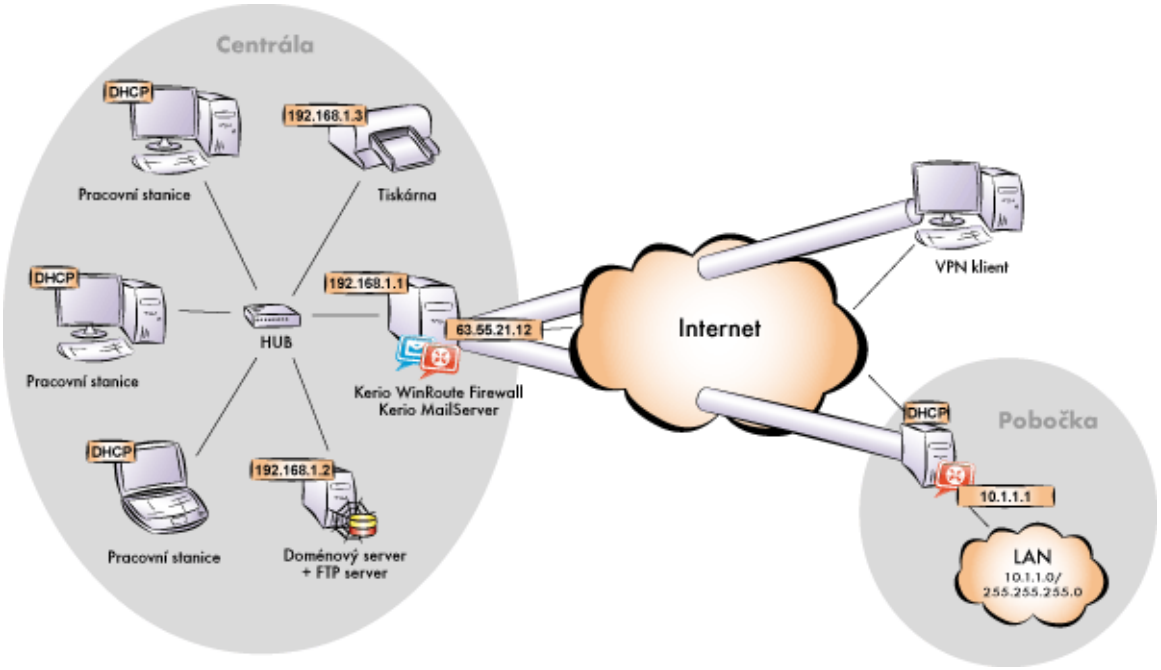
Nastavení IP adres v modelové síti

Počítačům v lokální síti přidělíme IP adresy následovně:

- Doménový server / FTP server bude mít statickou IP adresu `192.168.1.2` (zejména z důvodu mapování komunikace z Internetu se jeho IP adresa nesmí měnit).
- Síťová tiskárna bude mít pevnou IP adresu přidělovanou protokolem DHCP (rezervace v DHCP serveru). Tiskárna nemůže mít dynamickou IP adresu — kdyby se její adresa změnila, byla by pro klienty nedostupná.

Poznámka: V principu nezáleží na tom, zda je IP adresa tiskárny nastavena ručně nebo je tiskárně přidělována pevná adresa DHCP serverem. Při použití DHCP serveru odpadá konfigurace samotné tiskárny a její adresa je vidět v seznamu přidělených adres DHCP serveru. Naopak při ruční konfiguraci adresy bude tiskárna nezávislá na dostupnosti DHCP serveru.

- Pracovním stanicím v lokální síti budou přidělovány dynamické IP adresy (výrazně jednodušší konfigurace).



Obrázek 2.1 Modelová konfigurace sítě s přidělenými IP adresami

Poznámky:

1. DNS doména v lokální síti musí být shodná s doménou *Active Directory*, tj. `firma.cz`.

2. V síti pobočky firmy budou použity IP adresy `10.1.1.x` s maskou subsítě `255.255.255.0` a DNS doména `pobocka.firma.cz`.

2.2 Konfigurace síťových rozhraní internetové brány

Internetová brána je počítač (server), který spojuje lokální síť a Internet. Na tento počítač bude nasazen *WinRoute* (viz kapitola 2.3).

Rozhraní připojené do Internetu

Na rozhraní připojeném do Internetu nastavíme parametry TCP/IP dle informací od poskytovatele internetového připojení (ISP). Pro správnou funkci jsou nezbytně nutné tyto parametry: IP adresa, maska subsítě, výchozí brána a adresa alespoň jednoho DNS serveru.

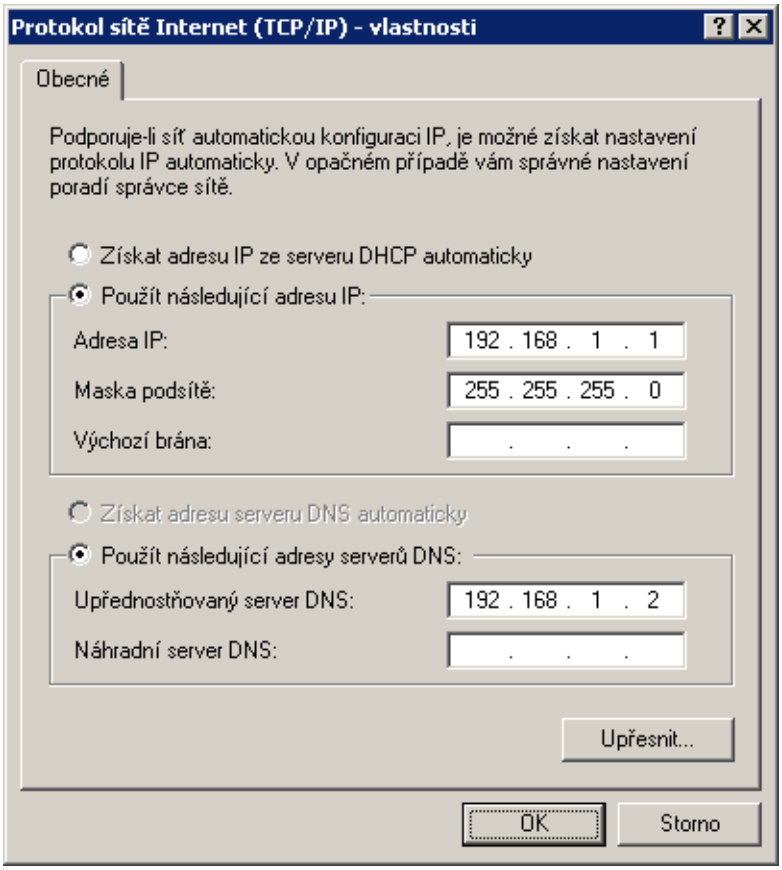
Internetové rozhraní firewallu v centrále firmy by mělo mít pevnou IP adresu, aby se k němu mohl připojovat server pobočky firmy a VPN klienti (viz požadavky v kapitole 1). Předpokládejme, že ISP přidělil IP adresu `63.55.21.12`. Rovněž je vhodné, aby této IP adrese bylo přiřazeno DNS jméno (např. `kwf.firma.cz`) — jinak by všichni VPN klienti museli zadávat server IP adresou.

Funkčnost internetového připojení prověříme např. příkazem `ping` nebo otevřením nějaké WWW stránky v prohlížeči.

Rozhraní připojené do lokální sítě

Na rozhraní připojeném do lokální sítě nastavíme tyto parametry:

- *IP adresa* — zvolíme IP adresu `192.168.1.1` (viz kapitola 2.1)
- *maska subsítě* — `255.255.255.0`
- *výchozí brána* — na tomto rozhraní nesmí být nastavena žádná výchozí brána!
- *DNS server* — pro správnou funkci ověřování v *Active Directory* musí být jako primární DNS server nastaven příslušný doménový server. Do položky *Upřednostňovaný DNS server* zadáme IP adresu doménového serveru (`192.168.1.2`).



Obrázek 2.2 Nastavení TCP/IP na rozhraní připojeném do lokální sítě

2.3 Instalace WinRoute

Na počítači, který je zapojen jako internetová brána (viz kapitola 2.1), spustíme instalační program *WinRoute*. Zvolíme *Úplnou* instalaci.

Pokud instalační program detekuje službu *Windows Firewall / Sdílení připojení k Internetu* (*Windows Firewall / Internet Connection Sharing*)[1], zobrazí dotaz, zda má být tato služba zakázána. Striktně doporučujeme tuto službu zakázat, jinak může docházet k nízkoúrovňovým kolizím a *WinRoute* nebude fungovat správně. Rovněž doporučujeme zakázat i další kolizní systémové služby — *Universal Plug and Play Device Host* a *SSDP Discovery Service*.

V závěru instalace se zobrazí průvodce počáteční konfigurací *WinRoute*, ve kterém nastavíme uživatelské jméno a heslo pro administrátorský přístup.

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

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

Obrázek 2.3 Instalace — detekce kolizních systémových služeb

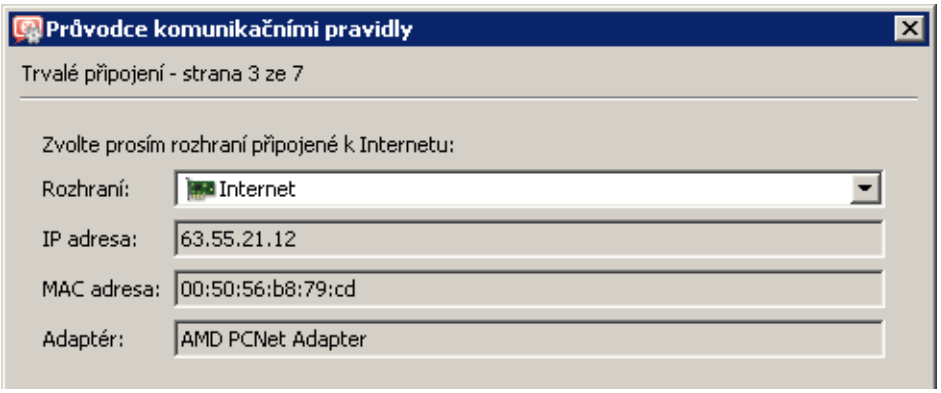
2.4 Základní nastavení komunikačních pravidel

Spustíme program *Kerio Administration Console* a přihlásíme se (použijeme jméno a heslo zadané při instalaci). Po prvním přihlášení se automaticky spustí *Průvodce komunikačními pravidly*.

V průvodci nastavíme:

- Typ internetového připojení (*Krok 2*) — zvolíme typ internetového připojení jednou pevnou linkou.
- Rozhraní připojené do Internetu (*Krok 3*) — vybereme adaptér připojený do Internetu.

Obrázek 2.4 Průvodce komunikačními pravidly — výběr typu internetového připojení

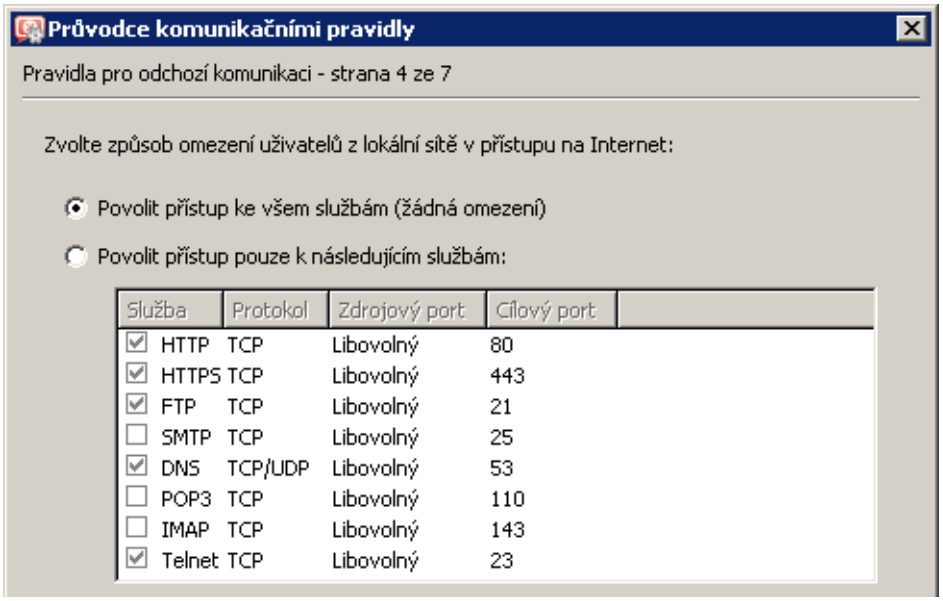


Obrázek 2.5 Průvodce komunikačními pravidly — výběr internetového rozhraní

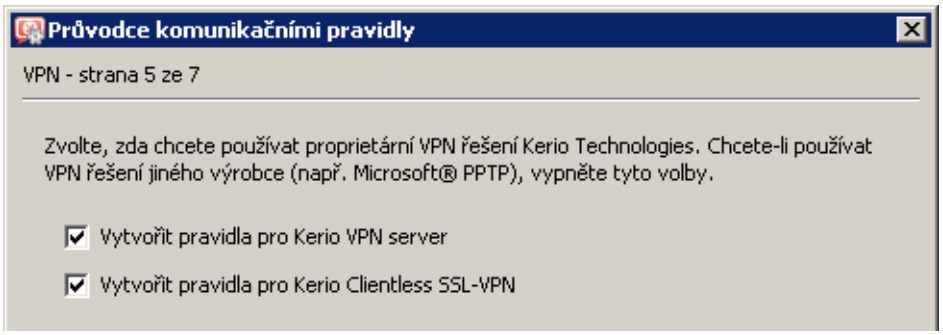
- Pravidla pro odchozí komunikaci (*Krok 4*) — povolíme přístup z lokální sítě ke všem službám v Internetu.

- Pravidla pro *Kerio VPN* (*Krok 5*) — zapneme volbu *Vytvořit pravidla pro Kerio VPN*. Tím budou vytvořena komunikační pravidla nutná pro propojení sítí centrály a pobočky a pro připojování vzdálených klientů (podrobnosti viz kapitola 4).

  Abychom umožnili vzdálený přístupa ke sdíleným složkám a souborům v síti prostřednictvím WWW prohlížeče, zapneme také volbu *Vytvořit pravidla pro Kerio Clientless SSL-VPN.*

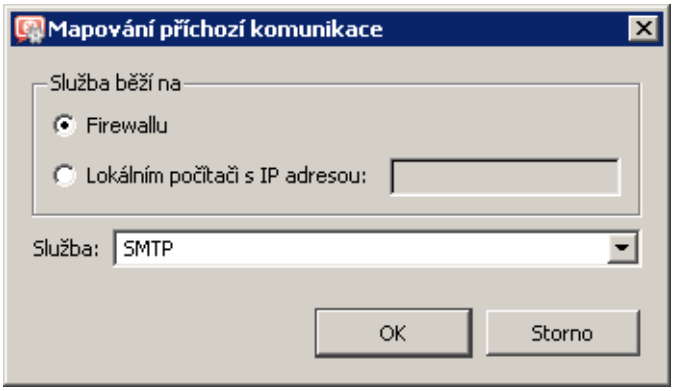


Obrázek 2.6 Průvodce komunikačními pravidly — pravidla pro odchozí komunikaci

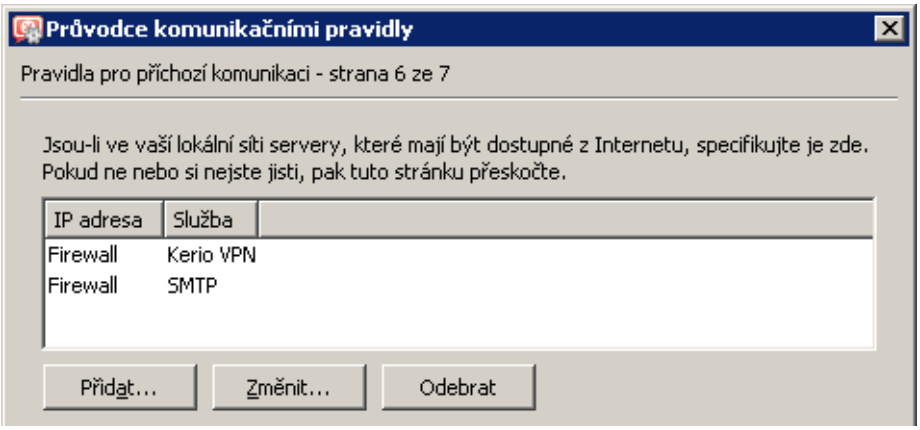


Obrázek 2.7 Průvodce komunikačními pravidly — pravidla pro Kerio VPN

- Pravidla pro příchozí komunikaci (*Krok 6*) — nastavíme mapování SMTP serveru na firewallu.



Obrázek 2.8 Průvodce komunikačními pravidly — mapování SMTP serveru



Obrázek 2.9 Průvodce komunikačními pravidly — pravidla pro příchozí komunikaci

Poznámka: V tomto kroku průvodce můžeme také nastavit mapování FTP serveru v lokální síti. Pro větší názornost však použijeme druhý způsob — definici vlastního komunikačního pravidla. Podrobnosti viz kapitola 2.13.

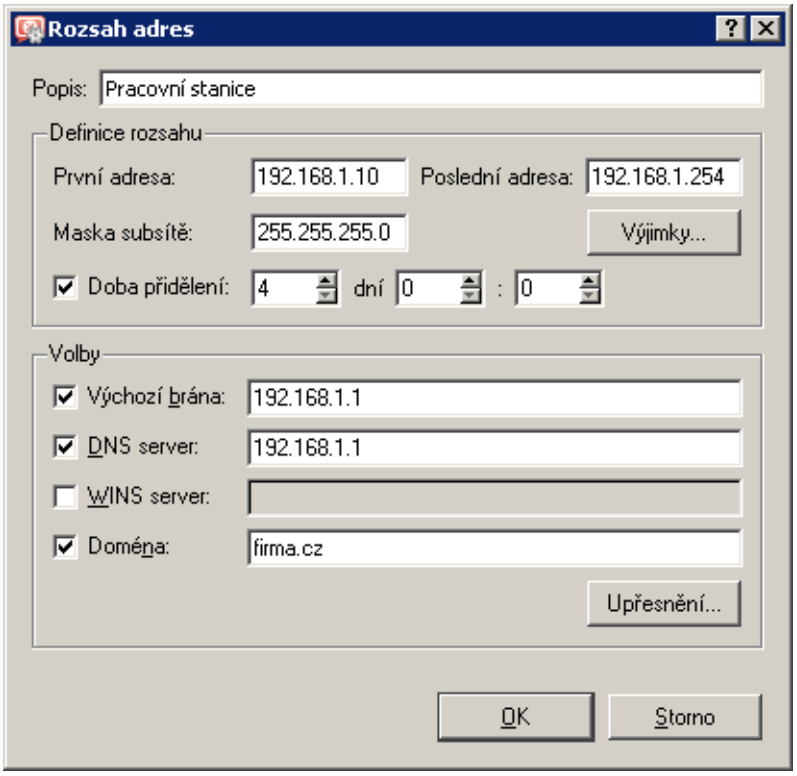
Poznámka: Na serveru pobočky nemá smysl vytvářet pravidla pro *Kerio VPN* a pro příchozí komunikaci (server má dynamickou veřejnou IP adresu a žádní klienti se k němu nemohou připojovat).

2.5 Nastavení DHCP serveru

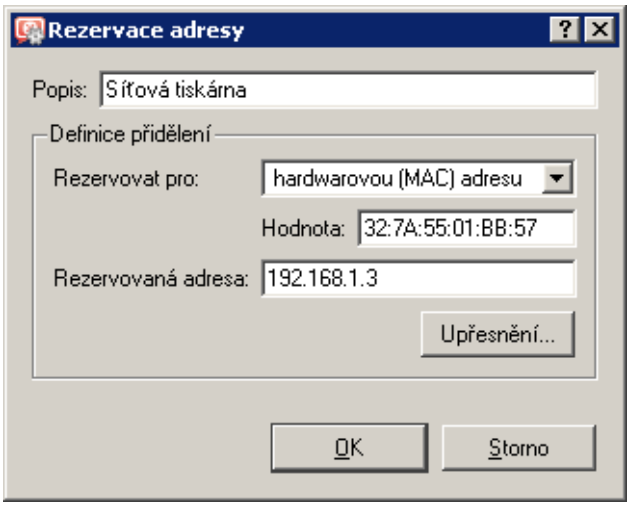
V programu *Kerio Administration Console* zvolíme sekci *Konfigurace* → *DHCP server*. Nejprve v záložce *Rozsahy adres* vytvoříme rozsah adres dynamicky přidělovaných pracovním stanicím (volba *Přidat* → *Rozsah adres...*). Při definici rozsahu je třeba specifikovat tyto parametry:

- *První adresa* — zvolíme `192.168.1.10` (IP adresy `192.168.1.1 - 192.168.1.9` zůstanou vyhrazeny pro servery a tiskárny),
- *Poslední adresa* — `192.168.1.254` (nejvyšší možná pro zvolenou subsíť),
- *Maska subsítě* — `255.255.255.0`,
- *Výchozí brána* — IP adresa rozhraní firewallu připojeného do lokální sítě (`192.168.1.1`).
- *DNS server* — IP adresa rozhraní firewallu připojeného do lokální sítě (stejně jako výchozí brána). Jako primární DNS server bude použit *DNS forwarder* ve *WinRoute*, který zajistí správné předávání dotazů mezi pobočkami firmy a do Internetu.

Dále volbou *Přidat* → *Rezervaci...* vytvoříme rezervaci pro síťovou tiskárnu. Rezervovaná IP adresa nemusí být z výše uvedeného rozsahu, musí ale náležet do zvolené subsítě (v tomto příkladu rezervujeme adresu `192.168.1.3`). Pro vytvoření rezervace je třeba znát hardwarovou (MAC) adresu tiskárny.



Obrázek 2.10 DHCP server — definice rozsahu IP adres pro pracovní stanice



Obrázek 2.11 DHCP server — rezervace IP adresy pro tiskárnu

Tip

Neznáte-li MAC adresu tiskárny, nevytvářejte rezervaci ručně. Po aktivaci DHCP serveru připojte tiskárnu do sítě. Tiskárně bude přidělena IP adresa z definovaného rozsahu (viz výše). V záložce *Přidělené IP adresy* tuto adresu označte a stiskněte tlačítko *Rezervovat...* — zobrazí se dialog pro rezervaci adresy, ve kterém bude již vyplněna příslušná MAC adresa. Doplňte požadovanou IP adresu, případně popis a stiskněte tlačítko *OK*. Pak tiskárnu restartujte. Po

restartu DHCP server tiskárně přidělí správnou IP adresu.

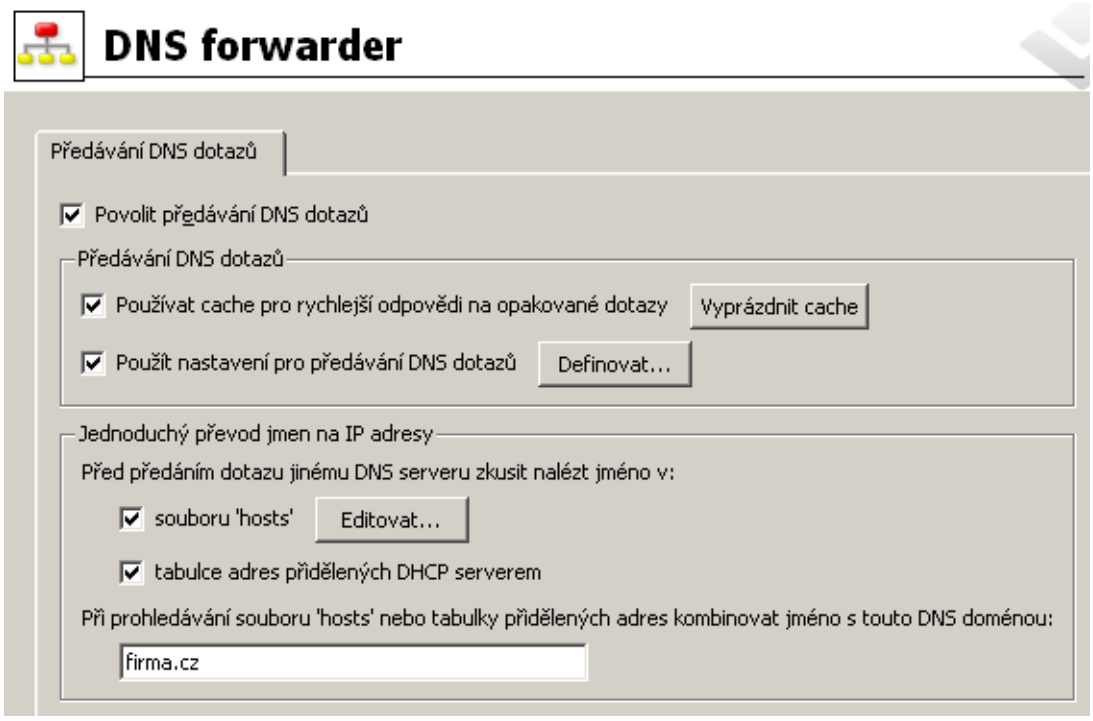
Poznámky:

1. DHCP server doporučujeme aktivovat až po definici všech požadovaných rozsahů a rezervací. Výjimkou je pouze případ, kdy potřebujeme zjistit MAC adresu klienta (viz výše).

2. Pro automatickou konfiguraci síťových zařízení lze použít i jiný DHCP server v lokální síti. V parametrech pro příslušný rozsah adres na tomto DHCP serveru nastavíme jako adresu výchozí brány a DNS serveru IP adresu rozhraní firewallu (tj. počítače s *WinRoute*) připojeného do lokální sítě.

2.6 Nastavení modulu DNS Forwarder

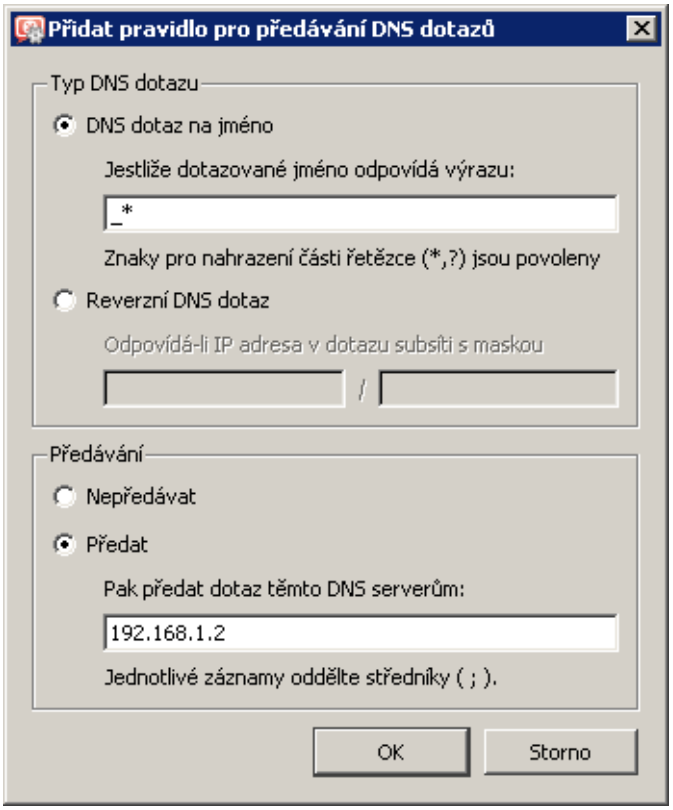
V sekci *Konfigurace* → *DNS forwarder* povolíme předávání DNS dotazů a nastavíme parametry modulu *DNS forwarder*:



Obrázek 2.12 Konfigurace modulu DNS Forwarder

- Volbu *Používat cache...* doporučujeme ponechat zapnutou (odezvy na opakované DNS dotazy budou výrazně rychlejší).

- Zapneme volbu *Použít nastavení pro předávání DNS dotazů*. Přidáme pravidlo pro předávání dotazů do *Active Directory*, tj. všech dotazů na jména začínající znakem _ (podtržítko), na doménový server v lokální síti — viz obrázek 2.13. Toto je nutné pro správnou komunikaci počítačů v lokální síti s doménovým serverem.



Obrázek 2.13 Předávání DNS dotazů do Active Directory

Dále bude potřeba přidat pravidla pro správné předávání dotazů mezi sítěmi centrály a pobočky firmy. Nastavení předávání DNS dotazů bude podrobně popsáno v kapitolách 4.1 a 4.2.

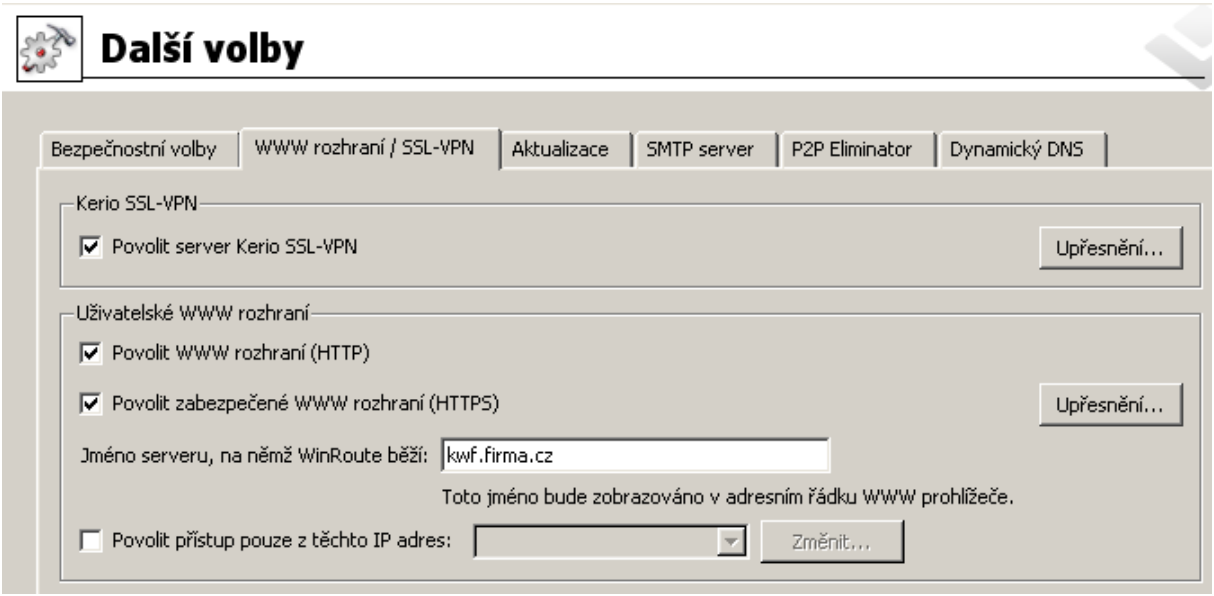
- Zapneme volby *souboru 'hosts'* a *tabulce adres přidělených DHCP serverem*. Spolupráce s DHCP serverem umožní, aby *DNS forwarder* dokázal zodpovědět dotazy na jména počítačů, které mají dynamicky přidělované IP adresy. Do souboru `hosts` pak můžeme ručně přidávat vlastní záznamy dle potřeby.

2.7 Nastavení WWW rozhraní a SSL-VPN

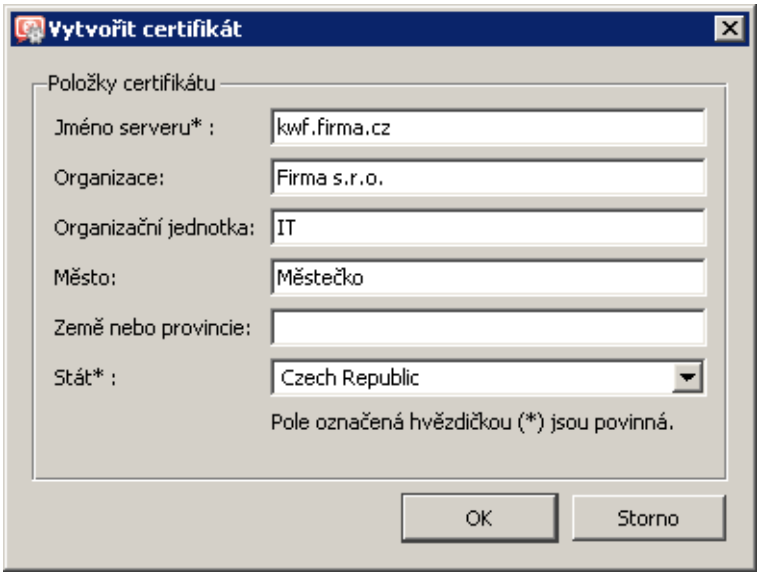
V sekci *Konfigurace* → *Další volby* → *WWW rozhraní / SSL-VPN* povolíme rozhraní *Clientless SSL-VPN* a WWW rozhraní *WinRoute*. Rozhraní *Clientless SSL-VPN* slouží pro zabezpečený vzdálený přístup ke sdíleným souborům v lokální síti prostřednictvím WWW prohlížeče. WWW rozhraní *WinRoute* je nutné pro zobrazování informací o zákazech při pokusu o přístup na zakázané WWW stránky (viz kapitola 2.10), zároveň jej uživatelé mohou využít pro nastavení některých parametrů uživatelského účtu nebo pro přístup ke statistikám.

V sekci *Kerio SSL-VPN* povolíme server rozhraní *Clientless SSL-VPN*. Volbou *Upřesnění* → *Změnit SSL certifikát* → *Vytvořit SSL certifikát* vytvoříme nový certifikát (podepsaný sám sebou) na jméno serveru `kwf.firma.cz`.

V sekci *Uživatelské WWW rozhraní* povolíme WWW rozhraní a stejným způsobem vytvoříme certifikát.



Obrázek 2.14 Nastavení parametrů Clientless SSL-VPN a WWW rozhraní



Obrázek 2.15 Vytvoření SSL certifikátu pro Clientless SSL-VPN a WWW rozhraní

Tip

Vytvořené certifikáty (které jsou podepsané samy sebou) můžeme později nahradit plnohodnotnými certifikáty vystavenými některou veřejnou certifikační autoritou.

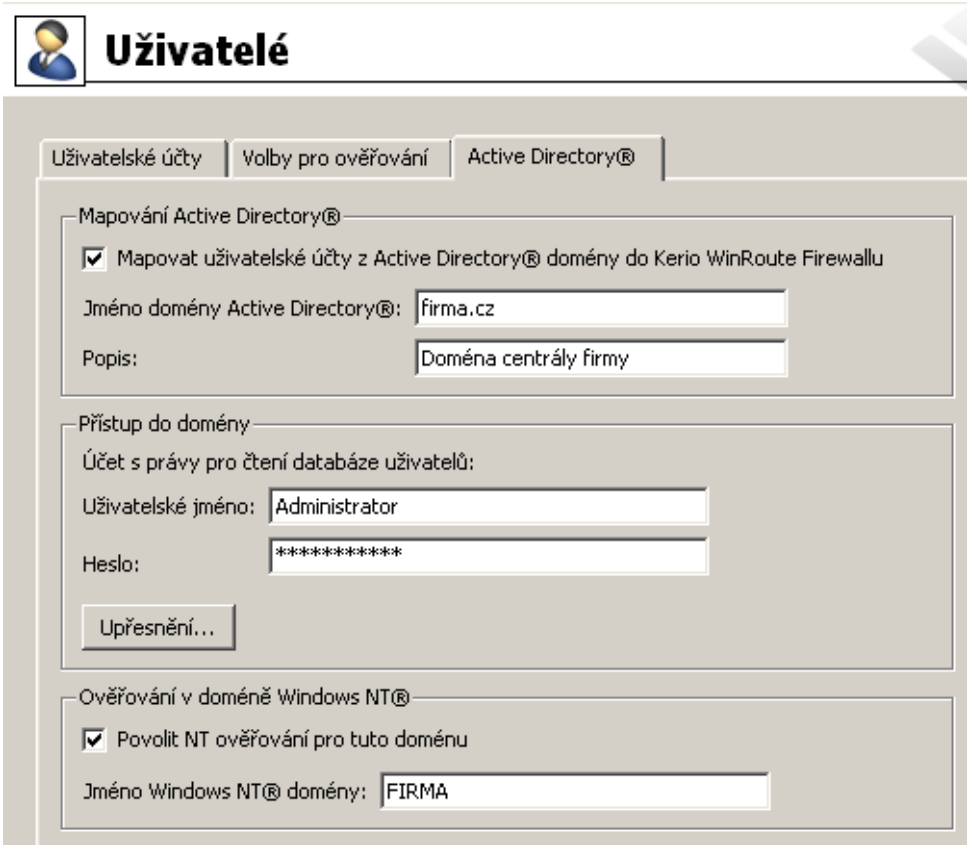
2.8 Mapování uživatelských účtů a skupin z Active Directory

Pro použití uživatelských účtů z *Active Directory* nastavíme mapování příslušné domény a definujeme šablonu, kterou nastavíme všem uživatelům parametry specifické pro *WinRoute* (uživatelská práva, kvóty objemu přenesených dat atd.).

Mapování domény

V lokální síti je vytvořena *Active Directory* doména. Ve *WinRoute* proto nemusíme definovat lokální uživatelské účty, stačí mapovat příslušnou doménu.

Mapování *Active Directory* domény nastavíme v sekci *Uživatelé a skupiny* → *Uživatelé*, záložka *Active Directory*.



Obrázek 2.16 Nastavení mapování Active Directory domény

Mapování Active Directory

Do položky *Jméno domény Active Directory* zadáme DNS jméno domény — *firma.cz*. Položka *Popis* slouží pouze pro snazší orientaci v *Administration Console*.

Přístup do domény

WinRoute potřebuje znát uživatelské jméno a heslo pro přístup do databáze *Active Directory*. K tomuto účelu stačí přístup pro čtení, tzn. můžeme použít libovolný uživatelský účet z příslušné domény.

Poznámka: Upřesňující parametry (tlačítko *Upřesnění*) není třeba nastavovat.

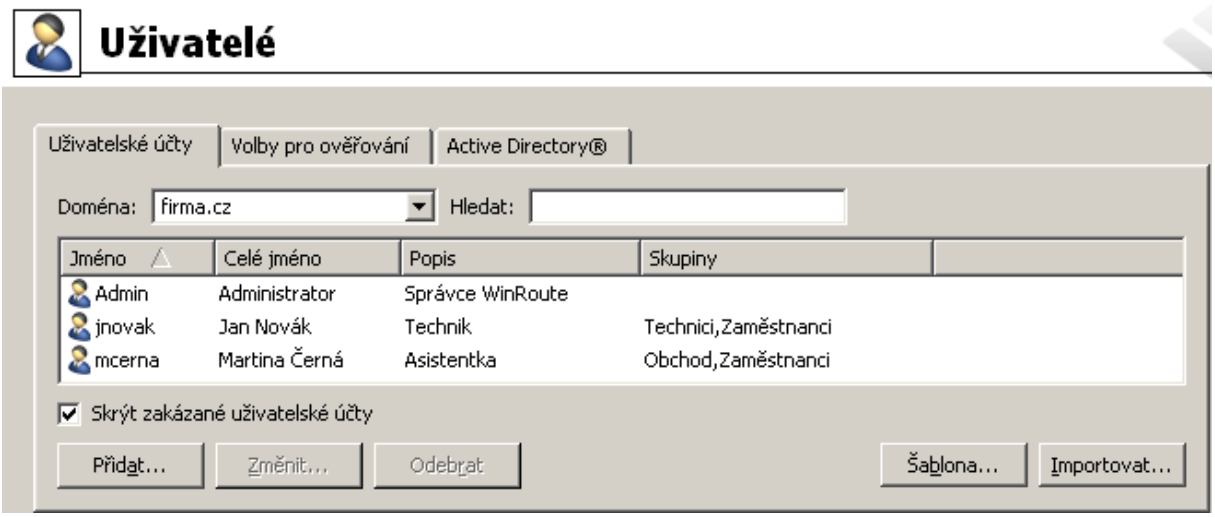
NT ověřování

Ověřování v doméně *Windows NT* je vhodné povolit — pro automatické ověřování uživatelů z WWW prohlížečů a pro zachování kompatibility se staršími verzemi *Windows*.

Do položky *Jméno NT domény* zadáme jméno odpovídající domény *Windows NT*, tj. `FIRMA`.

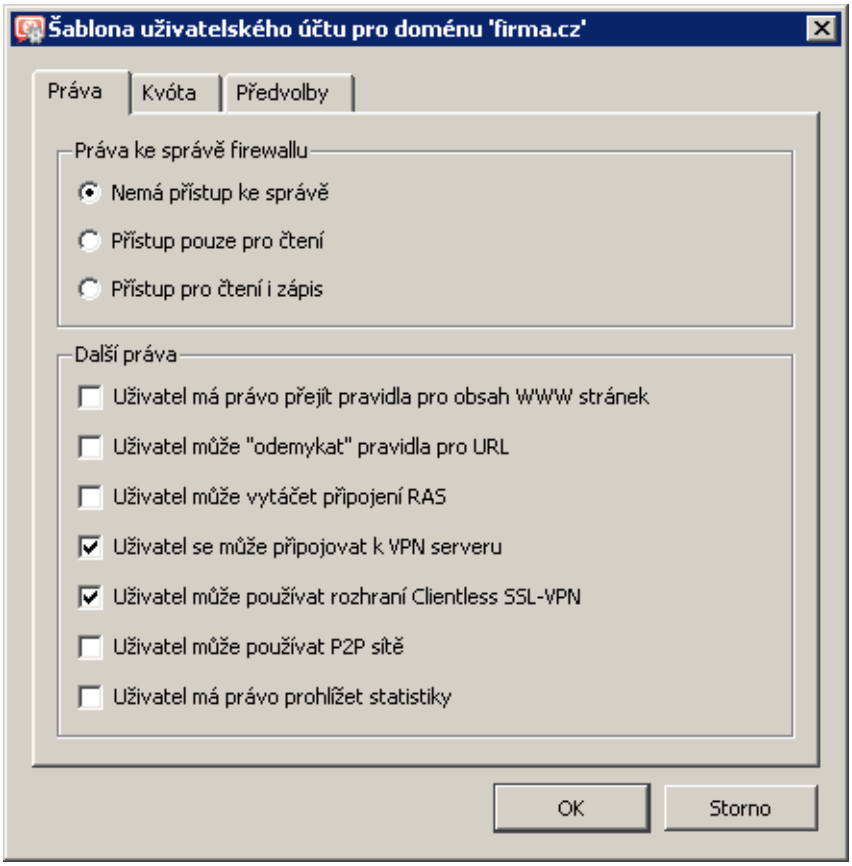
Definice šablony uživatelských účtů

V záložce *Uživatelské účty* vybereme mapovanou *Active Directory* doménu `firma.cz`.



Obrázek 2.17 Zobrazení uživatelských účtů v mapované doméně

Tlačítkem *Šablona* otevřeme dialog pro definici šablony uživatelských účtů. Požadavkem je umožnit uživatelům vzdálený přístup do lokální sítě prostřednictvím aplikace *Kerio VPN Client* nebo rozhraní *Clientless SSL-VPN* (viz kapitola 1). V záložce *Práva* nastavíme odpovídající uživatelská práva.

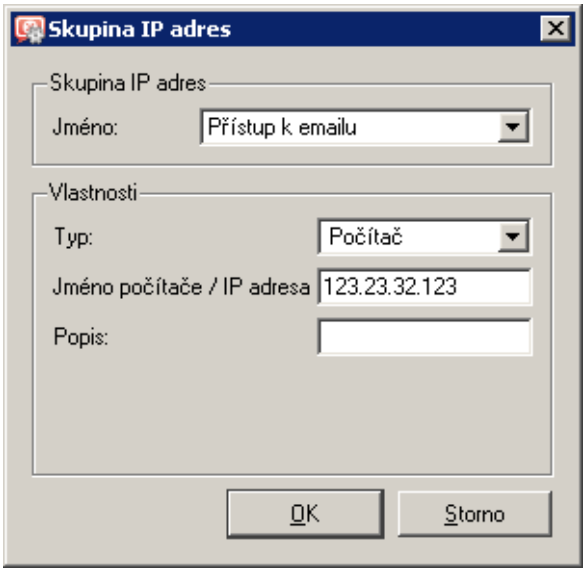


Obrázek 2.18 Šablona uživatelských účtů — práva pro Kerio VPN a Clientless SSL-VPN

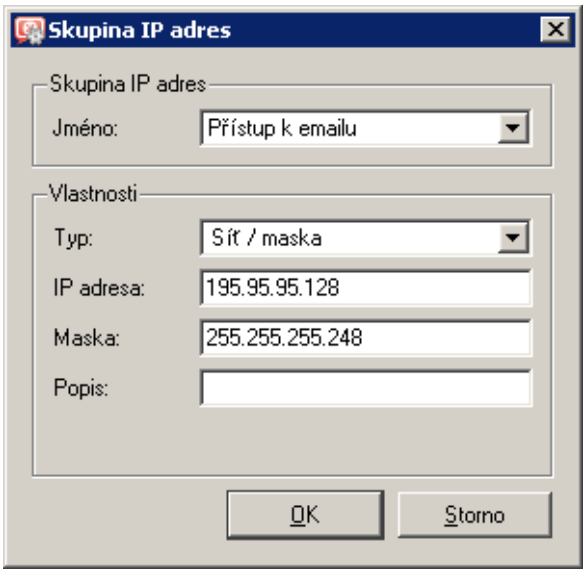
2.9 Skupiny IP adres a časové intervaly

V sekci *Definice* → *Skupiny IP adres* vytvoříme skupinu adres *Přístup k emailu*, kterou použijeme pro omezení přístupu k elektronické poště (viz kapitola 2.13). Tato skupina bude tvořena dvěma IP adresami `123.23.32.123`, `50.60.70.80` a celou subsítí `195.95.95.128` s maskou `255.255.255.248`.

Poznámka: Jméno musí být ve všech případech shodné, aby byly všechny položky zařazeny do jedné skupiny.

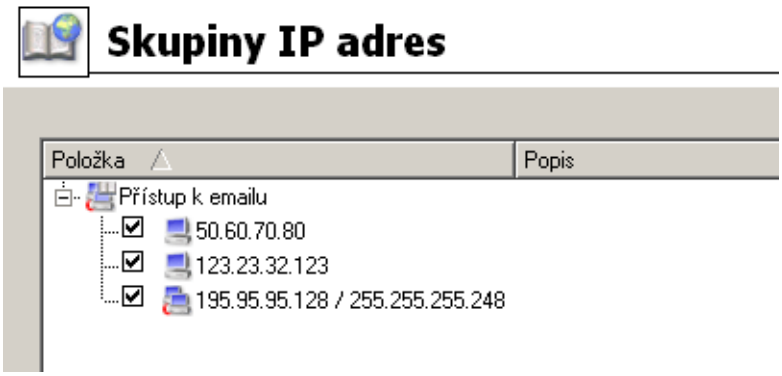


Obrázek 2.19 Skupina IP adres — přidání počítače

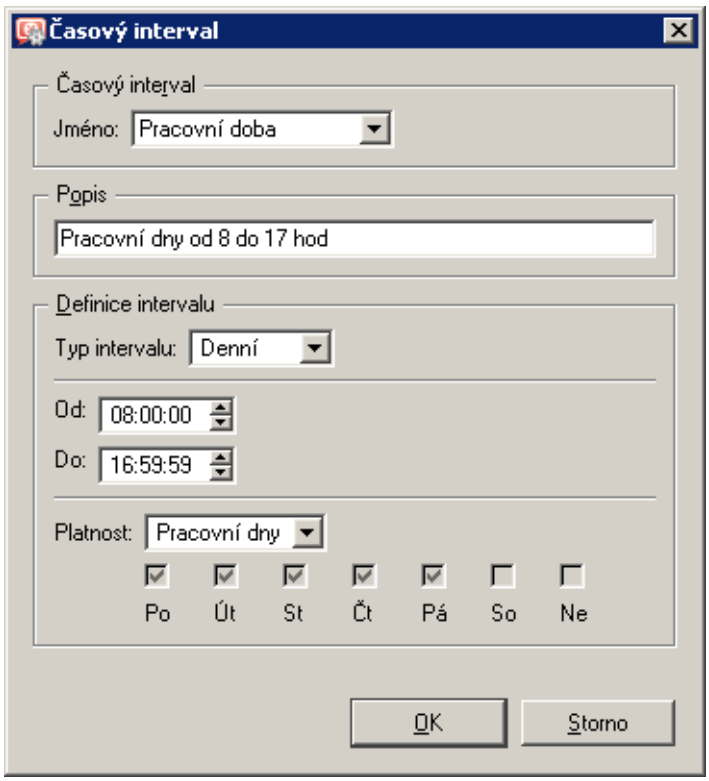


Obrázek 2.20 Skupina IP adres — přidání subsítě

V sekci *Definice* → *Časové intervaly* vytvoříme skupinu pro omezení přístupu v pracovní době (pondělí — pátek 8:00 — 16:30 hod., sobota a neděle 8:00 — 12:00 hod.).



Obrázek 2.21 Výsledná skupina IP adres

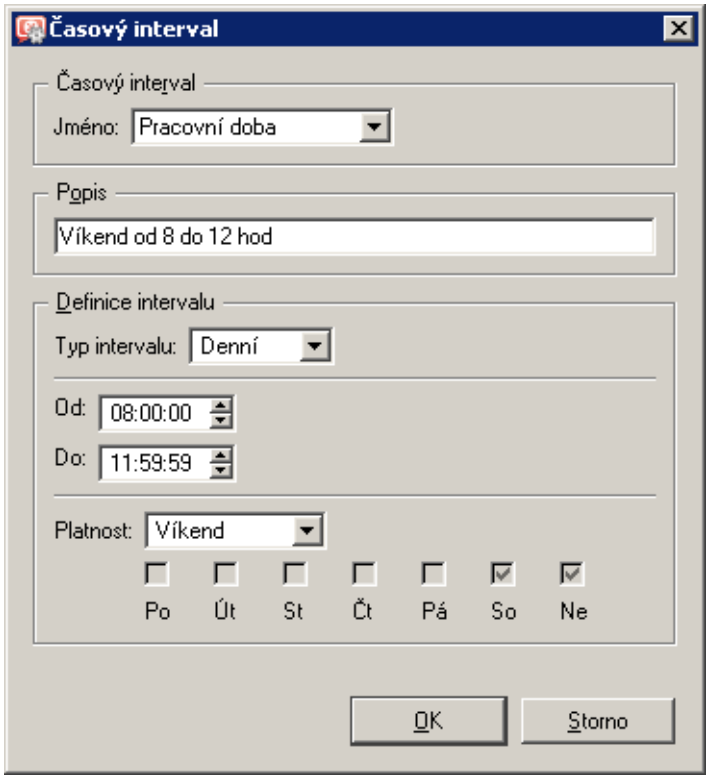


Obrázek 2.22 Definice pracovní doby ve dnech pondělí — pátek

Poznámky:

1. V obou případech můžeme v položce *Platnost* využít předdefinované skupiny dnů v týdnu (*Pracovní dny* a *Víkend*) — nemusíme zaškrtávat jednotlivé dny.

2. Položka *Jméno* musí být v obou případech stejná, aby došlo k vytvoření jednoho časového intervalu.



Obrázek 2.23 Definice pracovní doby o víkendu (sobota a neděle)

Obrázek 2.24 Výsledný časový interval Pracovní doba

2.10 Nastavení pravidel pro WWW

Požadavky

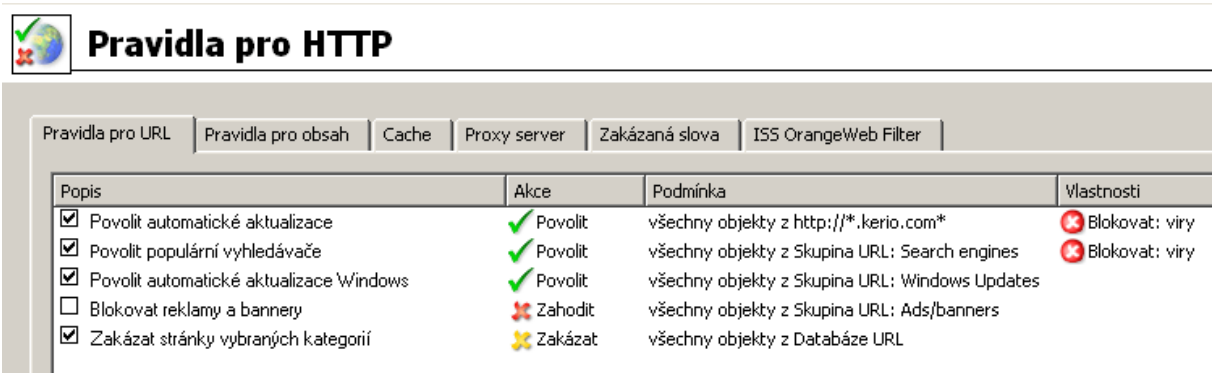
Přístup na WWW stránky má být omezen následujícím způsobem:

- filtrování reklam na WWW stránkách
- zákaz přístupu na stránky s erotickým obsahem

- zákaz přístupu na stránky s nabídkou pracovních míst, tyto stránky musejí zůstat přístupné členům personálního oddělení
- při přístupu na WWW bude vyžadováno ověření uživatele (lze tak lépe sledovat, jaké stránky kteří uživatelé navštěvují)

Předdefinovaná pravidla

V sekci *Konfigurace* → *Filtrování obsahu* → *Pravidla*, záložka *Pravidla pro URL* můžeme využít předdefinovaná základní pravidla:

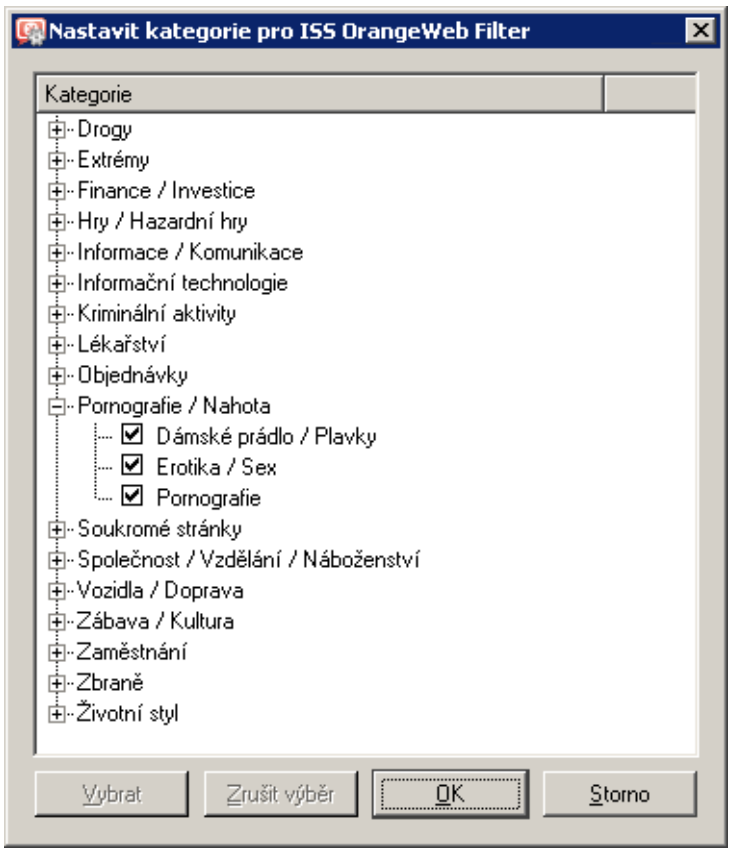


Obrázek 2.25 Předdefinovaná pravidla pro filtrování WWW stránek

- Pravidla *Povolit automatické aktualizace* a *Povolit automatické aktualizace Windows* doporučujeme ponechat zapnutá, aby fungovaly automatické aktualizace *WinRoute* a operačního systému serveru.
- Pravidla *Povolit populární vyhledávače* a *Blokovat reklamy a bannery* můžeme použít dle uvážení.
- Pravidlo *Zakázat stránky vybraných kategorií* můžeme využít k blokování přístupu na stránky s erotickým obsahem všem uživatelům.

  V definici pravidla musíme (tlačítkem *Vybrat hodnocení...*) zvolit kategorie, které chceme blokovat. Pro zakázání přístupu na stránky s erotickým obsahem zaškrtneme kategorie v sekci *Pornografie /Nahota*.

  V záložce *Upřesnění* zadáme text, který se uživateli zobrazí při pokusu o přístup na zakázanou stránku, případně nastavíme přesměrování na jinou stránku.



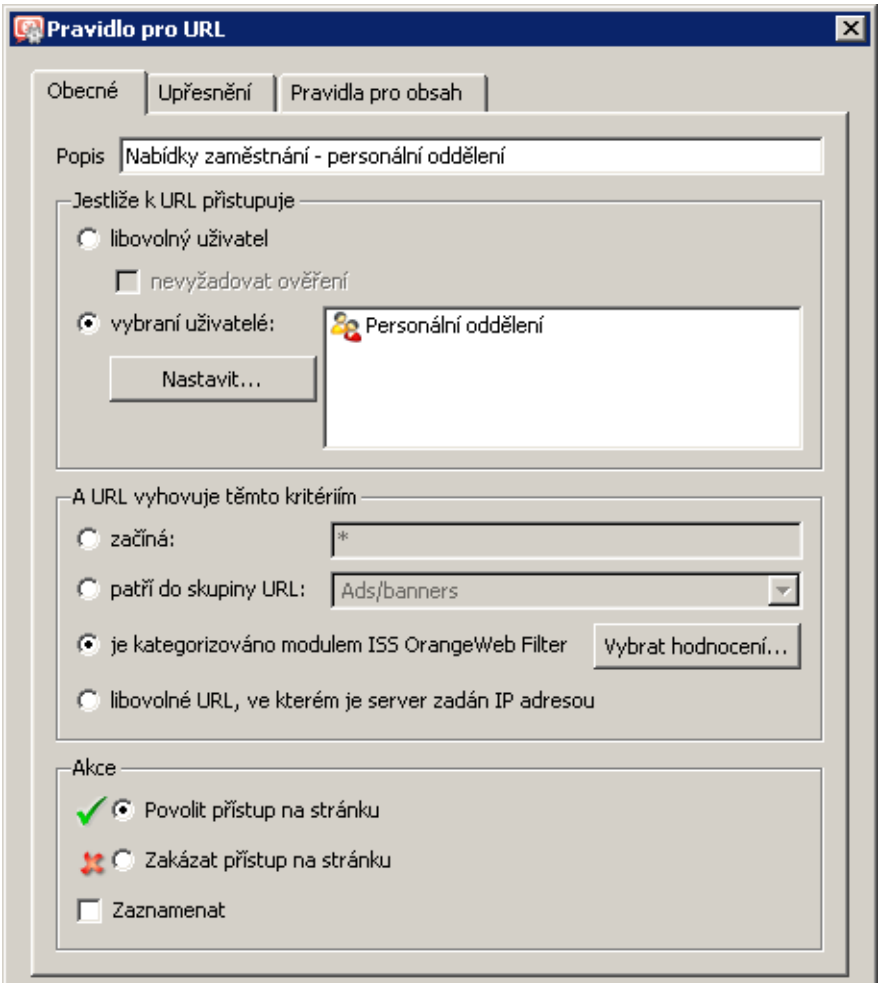
Obrázek 2.26 Výběr kategorií WWW stránek pro modul ISS OrangeWeb Filter

Definice vlastních pravidel

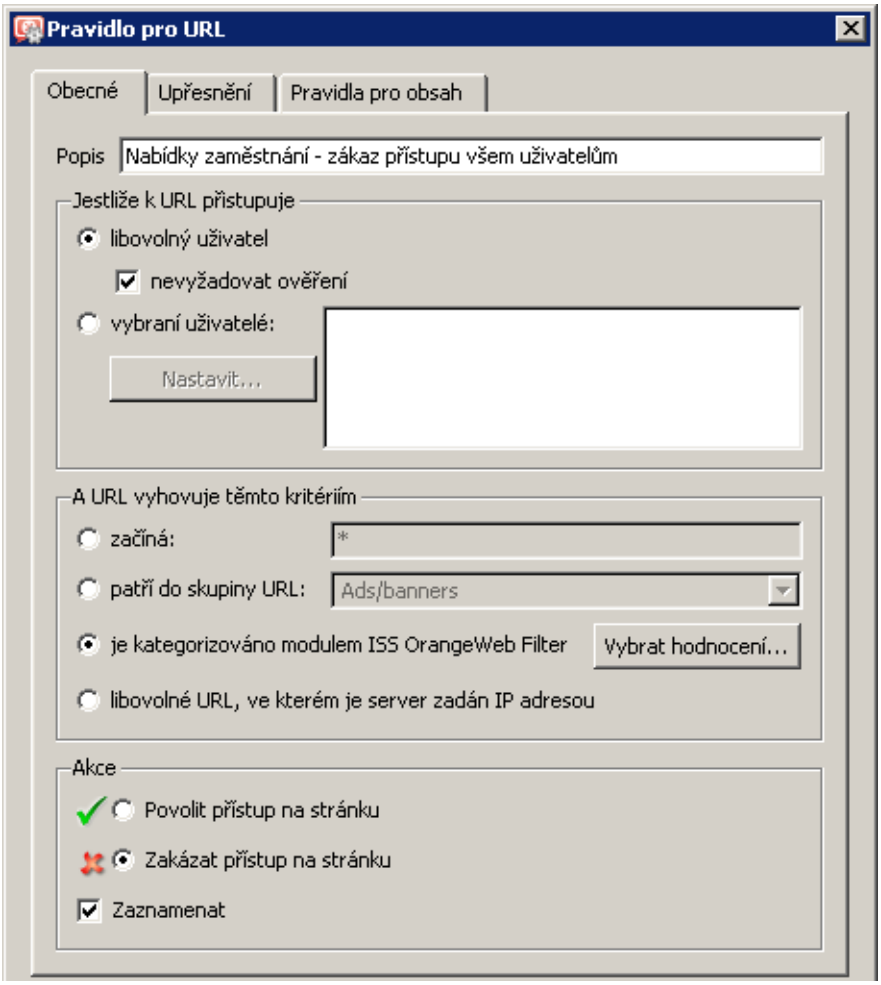
Omezení přístupu na WWW stránky s nabídkou pracovních míst realizujeme dvěma pravidly:

Přidáme pravidlo povolující přístup na stránky s nabídkou pracovních míst skupině uživatelů *Personální oddělení*.

Za toto pravidlo přidáme pravidlo zakazující přístup na stránky s nabídkou pracovních míst všem uživatelům.



Obrázek 2.27 Pravidlo pro URL — povolení přístupu na kategorii stránek skupině uživatelů

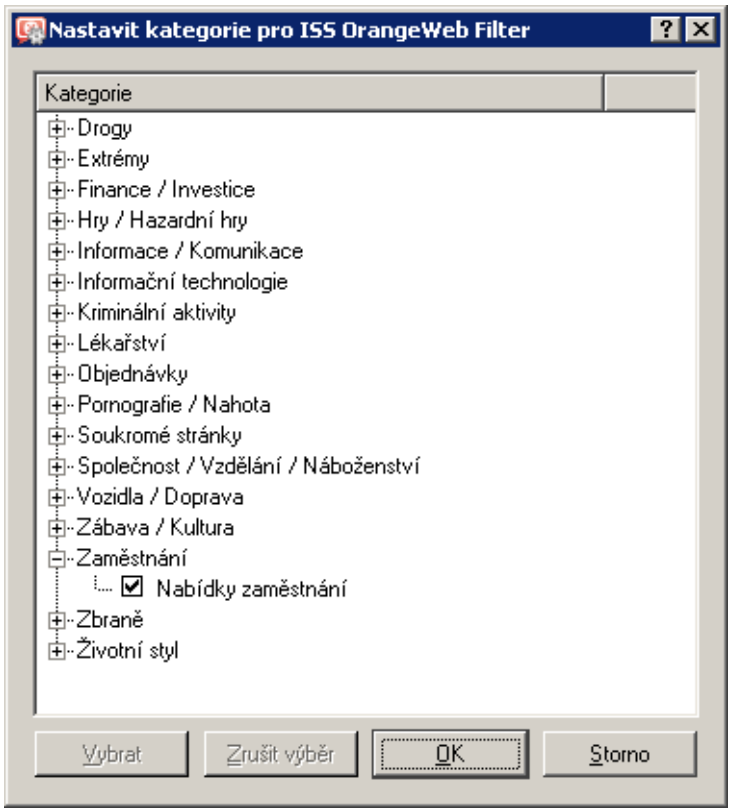


Obrázek 2.28 Pravidlo pro URL — zákaz přístupu na kategorii stránek všem (ostatním) uživatelům

Poznámky:

1. V pravidle zakazujícím přístup všem uživatelům je vhodné zapnout volbu *nevyžadovat ověření*. Tím zabráníme přesměrování uživatelů na přihlašovací stránku před zobrazením informace o zákazu.

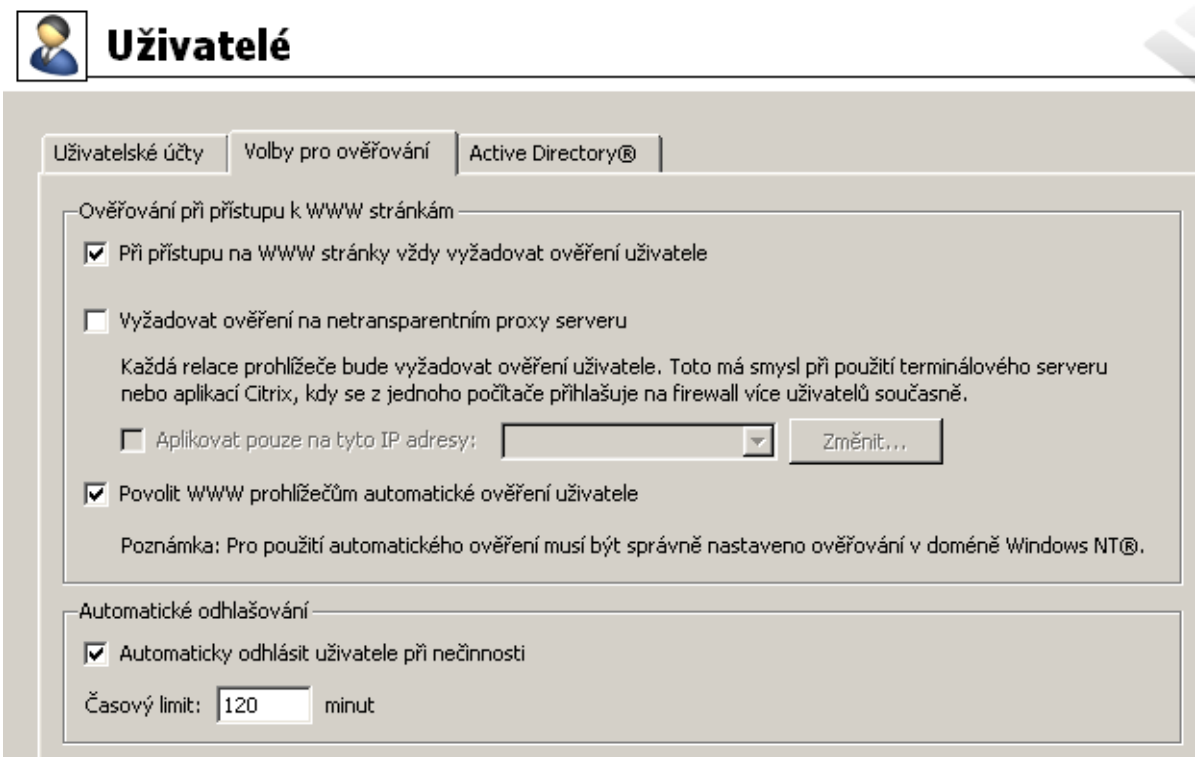
2. V obou pravidlech je vybrána jediná kategorie *Nabídky zaměstnání*.



Obrázek 2.29 Pravidlo pro URL — výběr kategorií WWW stránek

Vyžadování ověření uživatele při přístupu na WWW stránky

Posledním požadavkem omezení přístupu na WWW stránky je vyžadovat ověření uživatele při přístupu na libovolnou stránku. Tuto funkci aktivujeme v sekci *Uživatelé a skupiny* → *Uživatelé*, záložka *Volby pro ověřování*, volbou *Při přístupu na WWW stránky vždy vyžadovat ověření uživatele*.

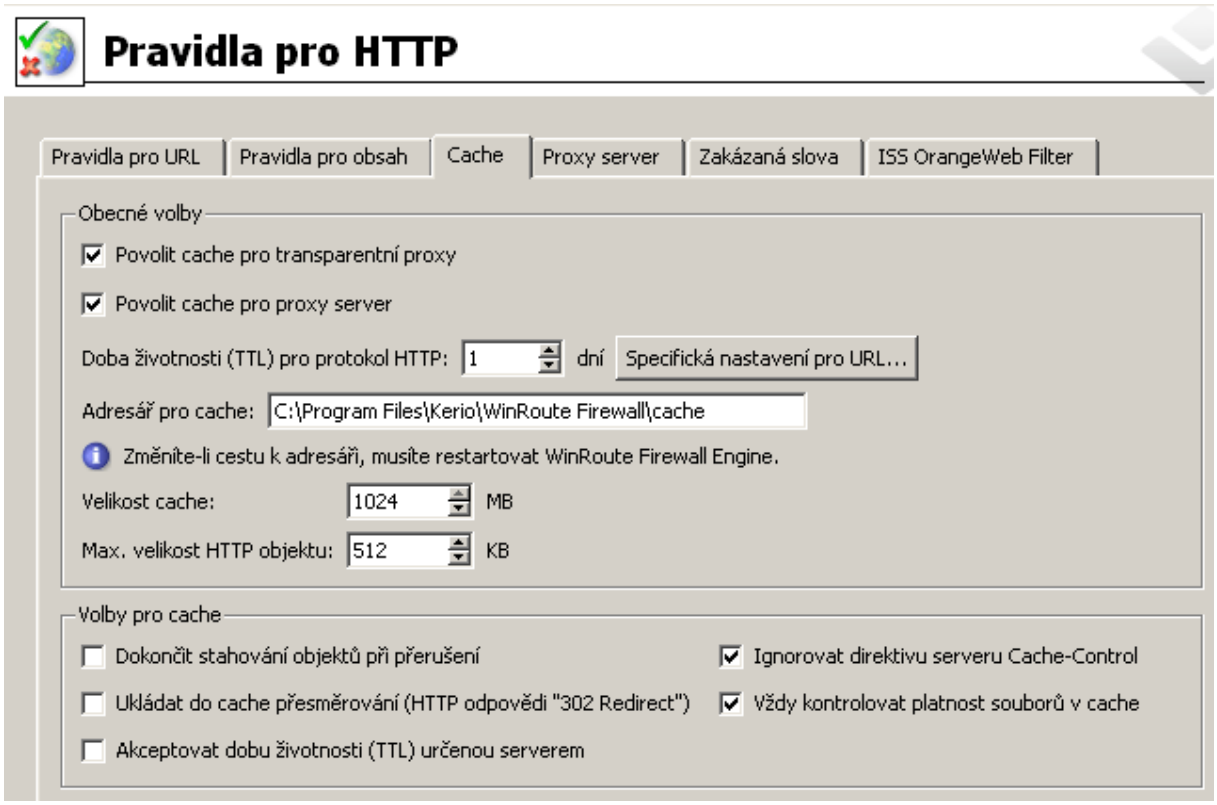


Obrázek 2.30 Vyžadování ověření uživatele při přístupu na WWW stránky

Nastavení HTTP cache

Cache slouží ke zrychlení přístupu na opakovaně navštěvované WWW stránky a snížení zatížení internetového připojení (v případě měřené linky se také sníží objem přenesených dat), proto ji doporučujeme použít. V sekci *Konfigurace* → *Filtrování obsahu* → *Pravidla pro HTTP*, záložka *Cache* zapneme volby *Povolit cache pro transparentní proxy* a *Povolit cache pro proxy server* (nezáleží na tom, zda jsou využity oba typy přístupu nebo pouze některý z nich).

V položce *Velikost cache* nastavíme velikost cache dle potřeby a s ohledem na velikost dostupného místa na disku. Výchozí hodnota je `1 GB` (`1024 MB`), maximum je téměř `2 GB` (`2047 MB`).



Obrázek 2.31 Konfigurace HTTP cache

2.11 Nastavení pravidel pro FTP

Požadavky

Používání FTP bude omezeno následujícím způsobem:

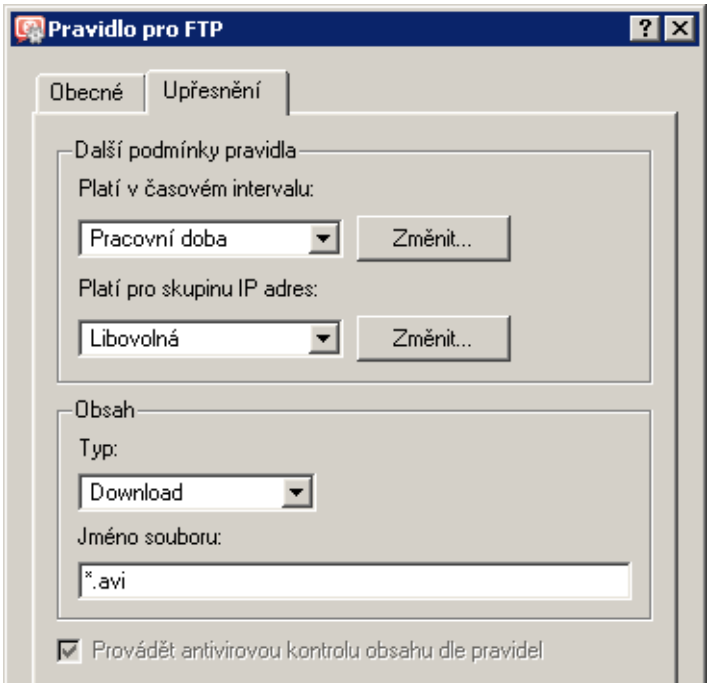
- zákaz přenosu hudebních souborů formátu MP3
- zákaz přenosu videa (`*.avi`) v pracovní době
- zákaz uploadu (ukládání souborů na FTP servery) — zabránění úniku informací z firmy

Předdefinovaná pravidla pro FTP

Omezení FTP nastavíme v sekci *Konfigurace* → *Filtrování obsahu* → *Pravidla pro FTP*. Pro všechna požadovaná omezení můžeme využít předdefinovaných pravidel:

- Pravidla *Zakázat soubory *.mpg, *.mp3 a *.mpeg* a *Zakázat upload* máme přímo k dispozici.
- Pravidlo *Zakázat soubory *.avi* upravíme tak, že v záložce *Upřesnění* zvolíme časový interval, ve kterém bude pravidlo platit.

Obrázek 2.32 Předdefinovaná pravidla pro FTP



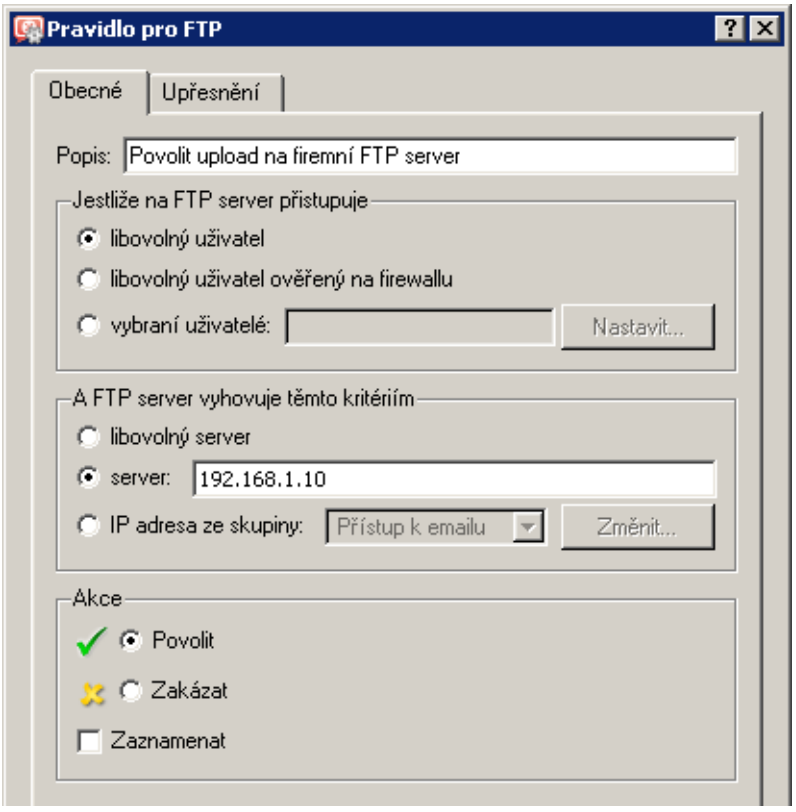
Obrázek 2.33 Pravidlo Forbid *.avi files — nastavení časové platnosti

- Doporučujeme zapnout také pravidlo *Zakázat resume z důvodu antivirové kontroly*, aby mohly být všechny soubory přenášené protokolem FTP důsledně kontrolovány antivirovým programem.

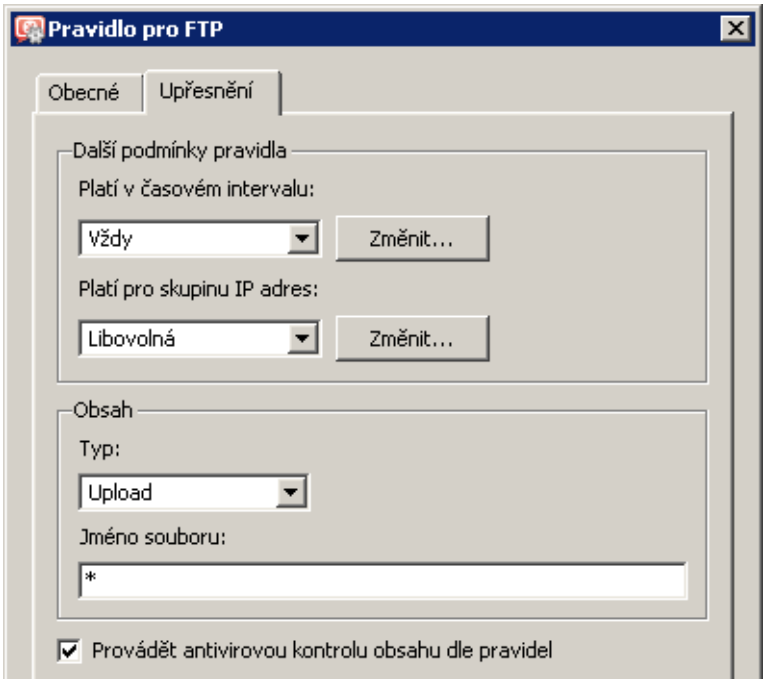
Upozornění

Pravidla pro FTP se vztahují na všechnu komunikaci protokolem FTP, která je obsluhována inspekčním modulem FTP.

V našem příkladu chceme zpřístupnit z Internetu FTP server v lokální síti. Pravidlo *Forbid upload* zakazuje upload také na tento server, což není žádoucí. Proto musíme před pravidlo *Forbid upload* přidat pravidlo, které povoluje upload na tento FTP server.



Obrázek 2.34 Pravidlo pro FTP — povolení přístupu na firemní FTP server



Obrázek 2.35 Pravidlo pro FTP — povolení uploadu libovolného souboru

Poznámky:

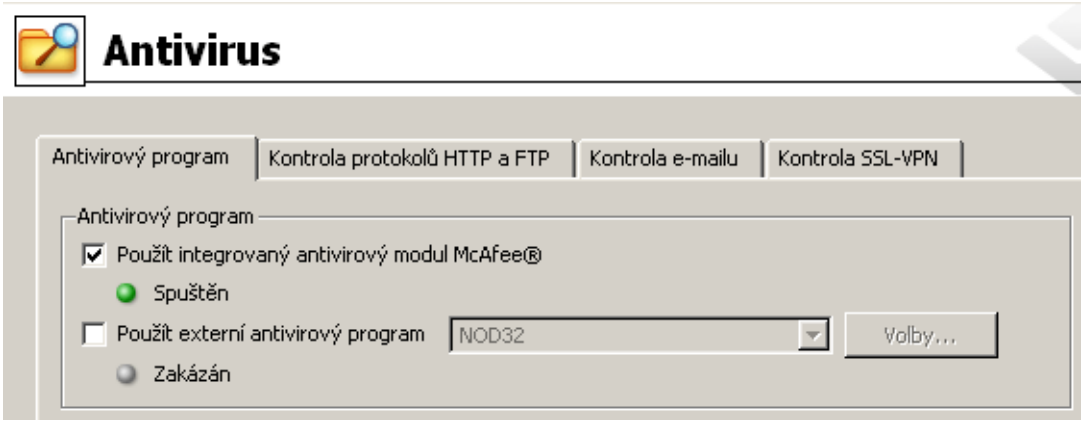
1. Jako IP adresa FTP serveru musí být uvedena adresa počítače v lokální síti, na kterém FTP server skutečně běží. Nelze uvést vnější IP adresu firewallu, z níž je FTP server mapován (pokud FTP server neběží přímo na firewallu)! Překlad IP adres se provádí před zpracováním pravidel pro filtrování obsahu.

2. Obdobným způsobem lze povolit i upload na konkrétní FTP server v Internetu, zatímco na všechny ostatní FTP servery bude zakázán.

2.12 Nastavení antivirové kontroly

Chceme-li použít některý z podporovaných externích antivirů, nainstalujeme jej. Antivirus *McAfee* je součástí *WinRoute* a pro jeho činnost je třeba pouze speciální licence.

V sekci *Konfigurace* → *Filtrování obsahu* → *Antivirus*, záložka *Antivirový program*, nastavíme požadovaný antivirus a vybereme protokoly, na které má být antivirová kontrola aplikována.



Obrázek 2.36 Nastavení antivirové kontroly

Záložky *Kontrola HTTP a FTP* a *Kontrola e-mailu* umožňují podrobnější nastavení parametrů pro kontrolu jednotlivých protokolů. Výchozí nastavení je zpravidla vyhovující.

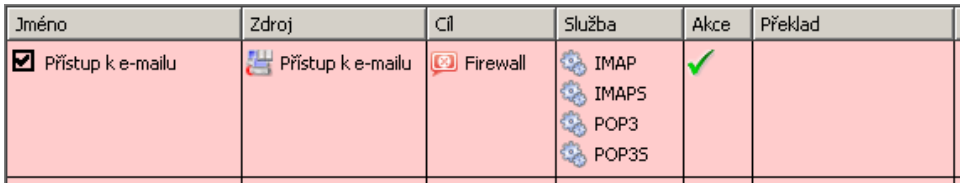
2.13 Zpřístupnění lokálních služeb z Internetu

V sekci *Konfigurace* → *Komunikační pravidla* přidáme pravidla pro služby, které mají být přístupné z Internetu. Pravidla pro mapování služeb by měla být umístěna vždy na začátku tabulky komunikačních pravidel.

- Zpřístupnění (mapování) lokálního FTP serveru — předpokládáme pouze nezabezpečený přístup, aby bylo možné komunikaci filtrovat a provádět antivirovou kontrolu.

Obrázek 2.37 Zpřístupnění lokálního FTP serveru z Internetu

- Přístup ke službám poštovního serveru (kromě SMTP) — povolíme pouze z požadovaných IP adres.



Obrázek 2.38 Povolení přístupu ke službám poštovního serveru na firewallu

Poznámky:

1. Toto pravidlo povoluje přístup ke službám *IMAP* i *POP3* v zabezpečené i nezabezpečené verzi — klienti si mohou vybrat, jakou službu budou využívat.

2. Služba SMTP byla mapována pomocí průvodce komunikačními pravidly (viz kapitola 2.4) — příslušné pravidlo v tomto okamžiku již existuje.

3. Poslat e-mail do lokální domény smí kdokoliv, proto nelze ke službě *SMTP* omezovat přístup pouze z určitých IP adres.

2.14 Zabezpečený přístup vzdálených klientů do lokální sítě

Pro zabezpečený přístup vzdálených klientů do lokální sítě (dále jen „VPN klienti“) povolíme VPN server v sekci *Konfigurace* → *Rozhraní*, záložka *Rozhraní* (podrobnosti viz kapitola 4.1). Žádná další nastavení nejsou třeba. Komunikace VPN klientů je již povolena pravidly vytvořenými průvodcem — viz kapitola 2.4.

Poznámky:

1. Pro připojení k VPN serveru ve *WinRoute* musí být na každém vzdáleném klientovi nainstalována aplikace *Kerio VPN Client*. Klienti se budou připojovat k serveru v centrále firmy (tj. na IP adresu `63.55.21.12`, resp. na jméno serveru `kwf.firma.cz`) a ověřovat uživatelským jménem a heslem svého účtu ve *WinRoute* (viz kapitola 2.8).

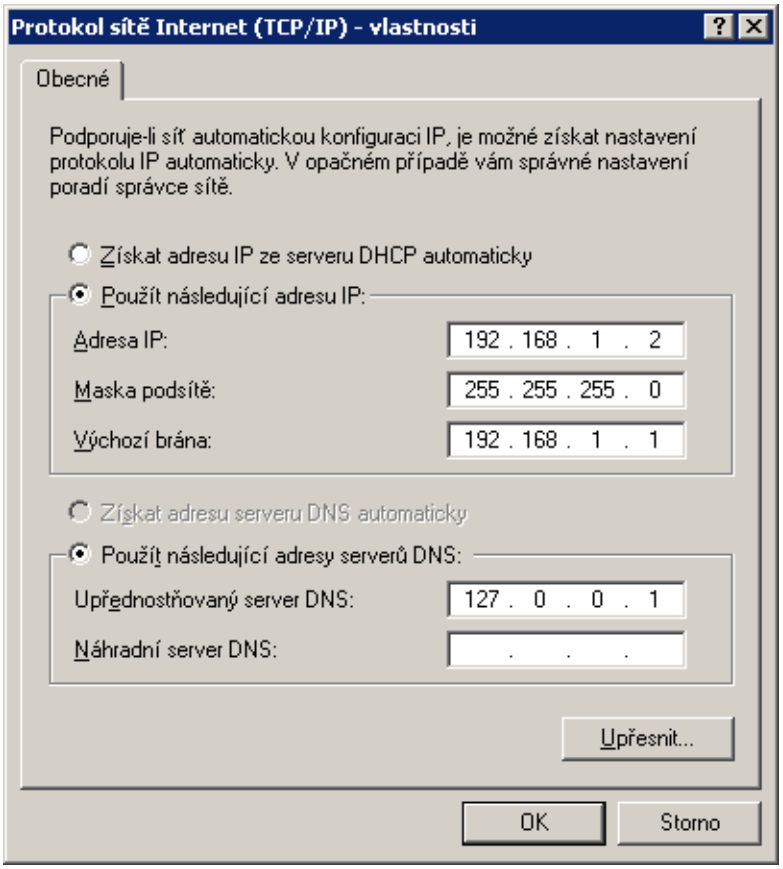
   Podrobné informace naleznete v manuálu *Kerio VPN Client — Příručka uživatele* (`http://www.kerio.cz/kwf-manual`).

2. VPN klienti se budou připojovat pouze na server v centrále firmy. Na serveru pobočky není třeba žádná nastavení pro VPN klienty provádět.

2.15 Nastavení počítačů v lokální síti

Na počítači, který slouží jako doménový server a FTP server, nastavíme parametry TCP/IP ručně (jeho IP adresa se nesmí měnit):

- *IP adresa* — zadáme adresu `192.168.1.2` (viz kapitola 2.5),
- *Výchozí brána* — zadáme IP adresu příslušného rozhraní firewallu, tj. `192.168.1.1`,
- *DNS server* — protože na tomto počítači běží *Microsoft DNS*, systém automaticky nastaví jako primární DNS server lokální zpětnovazební adresu (*loopback* — `127.0.0.1`).



Obrázek 2.39 Konfigurace TCP/IP na souborovém/FTP serveru

Na pracovních stanicích nastavíme automatickou konfiguraci IP adresy i DNS serveru pomocí DHCP (ve většině operačních systémů výchozí nastavení po instalaci).

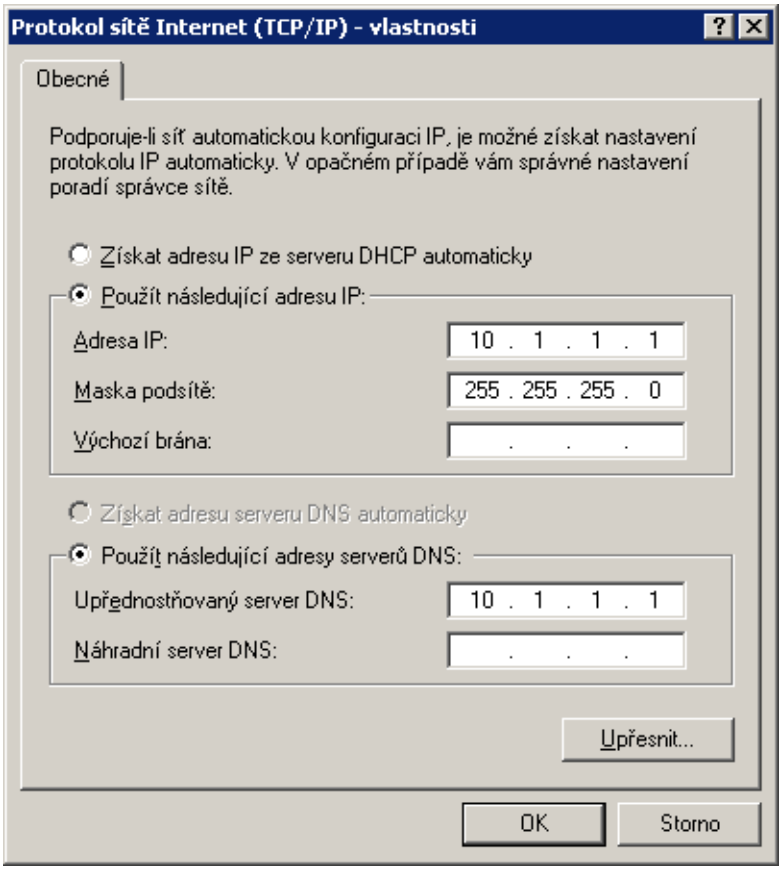
Kapitola 3

Konfigurace sítě v pobočce firmy

Pro rychlou konfiguraci sítě v pobočce firmy lze použít analogický postup jako pro síť centrály — viz kapitola 2. Jediný rozdíl je v konfiguraci DNS. Předpokládejme, že v síti pobočky firmy není doménový server ani žádný jiný DNS server. Funkci primárního DNS serveru zde bude plnit *DNS Forwarder* ve *WinRoute*.

3.1 Konfigurace síťových rozhraní internetové brány

Na rozhraní firewallu připojeném do lokální sítě nastavíme pevnou IP adresu (např. `10.1.1.1`). Stejnou IP adresu zadáme jako primární DNS server (aby DNS dotazy z lokálního počítače byly rovněž předávány *DNS Forwarderu* — důležité zejména v případě vytáčeného připojení). Na tomto rozhraní nesmí být nastavena žádná výchozí brána!

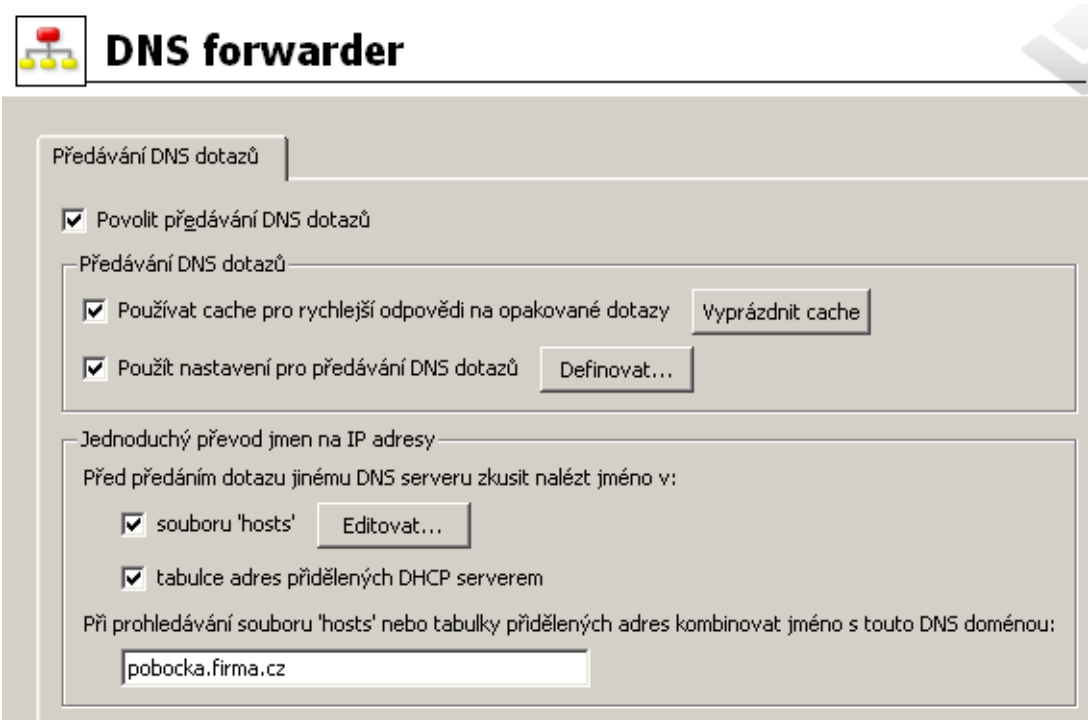


Obrázek 3.1 Pobočka — konfigurace lokálního rozhraní firewallu

Rozhraní připojené do Internetu nastavíme dle údajů od poskytovatele internetového připojení.

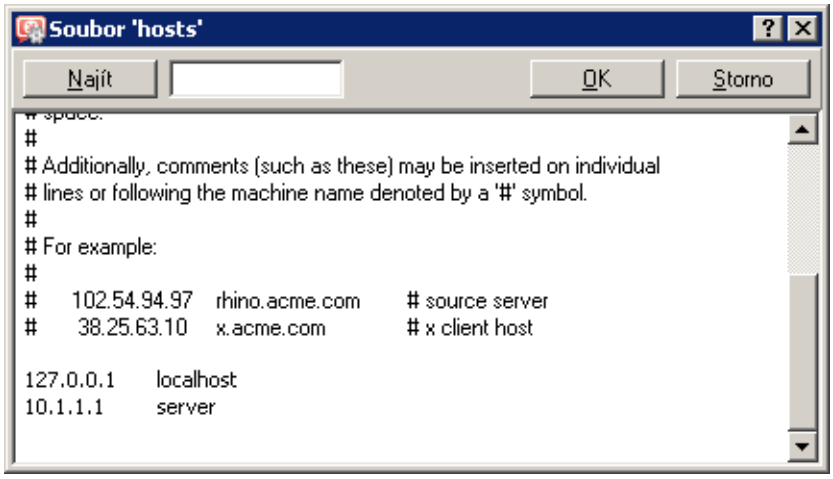
3.2 Nastavení DNS Forwarderu

V konfiguraci modulu *DNS Forwarder* zapneme jednoduchý převod DNS jmen. Do položky *Při prohledávání souboru 'hosts'...* uvedeme lokální doménu pobočky firmy, tj. `pobocka.firma.cz`.



Obrázek 3.2 Pobočka — konfigurace modulu DNS Forwarder

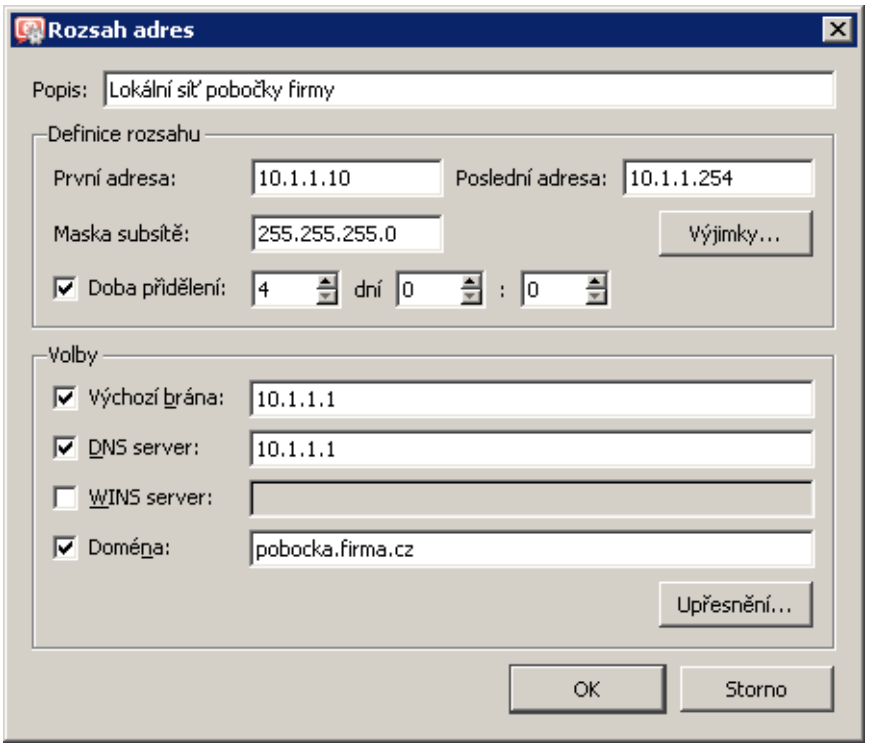
Do souboru *hosts* je vhodné přidat záznam o serveru (případně o dalších počítačích, kterým bude nastavena pevná IP adresa).



Obrázek 3.3 Pobočka — přidání záznamu o serveru do souboru 'hosts'

3.3 Nastavení DHCP serveru

V konfiguraci DHCP serveru nastavíme rozsah IP adres pro počítače v lokální síti pobočky. Jako adresu výchozí brány DNS serveru zadáme IP adresu lokálního rozhraní firewallu pobočky (`10.1.1.1`).



Obrázek 3.4 Pobočka — nastavení rozsahu adres přidělovaných DCHP serverem

Kapitola 4

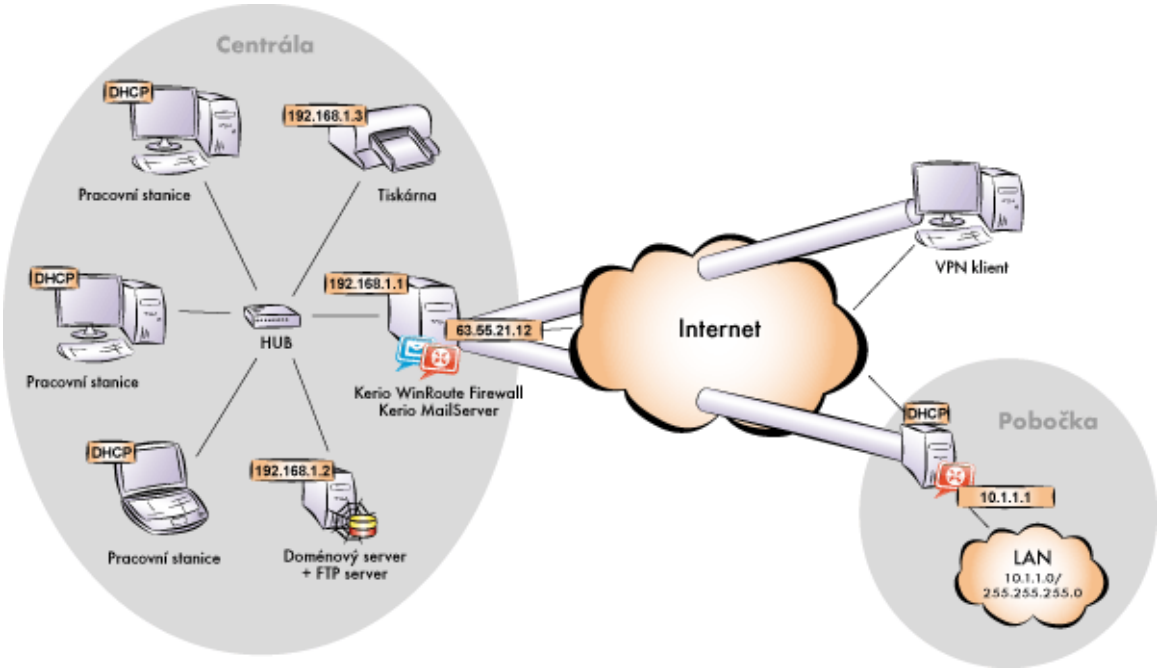
Propojení sítí centrály a pobočky

V této kapitole naleznete postup propojení sítí v centrále a v pobočce firmy zabezpečeným šifrovaným kanálem (dále jen „VPN tunel“). Příklad obsahuje pouze základní kroky pro vytvoření VPN tunelu mezi dvěma sítěmi — bez omezování přístupu a dalších specifických nastavení. Příklad složitější konfigurace VPN naleznete v manuálu *Kerio WinRoute Firewall — Příručka administrátora*.

Postup konfigurace je rozdělen na dvě části: nastavení v centrále firmy a nastavení v pobočce firmy. Předpokládejme, že obě sítě jsou již nastaveny podle postupu uvedeného v kapitole 2 a internetové připojení na obou stranách je funkční.

Informace k příkladu

Pro přehlednost uveďme znovu schéma propojovaných sítí včetně IP adres.



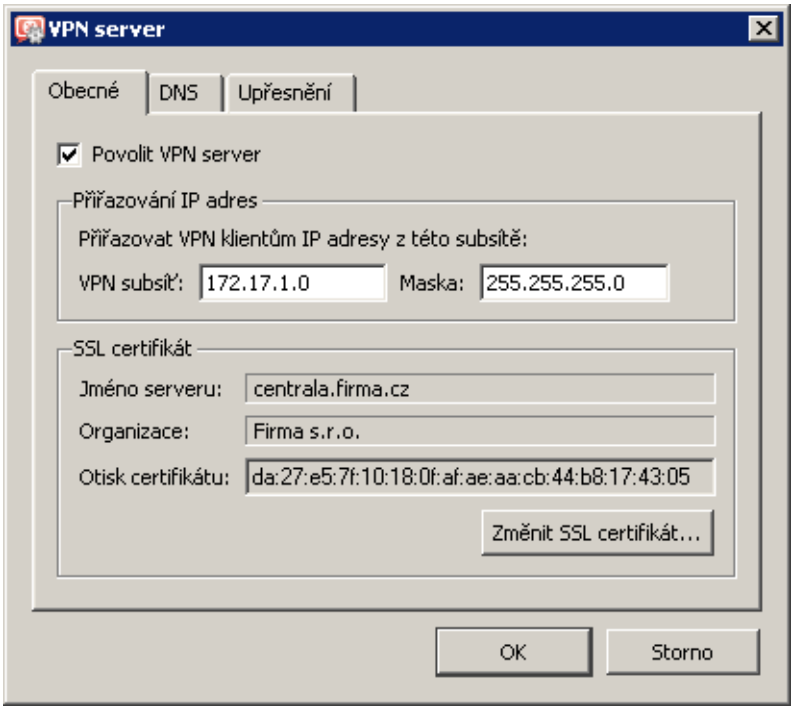
Obrázek 4.1 Modelová konfigurace sítě s přidělenými IP adresami

V centrále firmy jsou použity IP adresy `192.168.1.x` s maskou subsítě `255.255.255.0` a DNS doménu `firma.cz`. Pobočka používá IP adresy `10.1.1.x` s maskou subsítě `255.255.255.0` a subdoménu `pobocka.firma.cz`.

4.1 Konfigurace v centrále firmy

1. Ve *WinRoute* v sekci *Konfigurace / Rozhraní*, záložka *Rozhraní* vybereme *VPN server*. Dvojitým kliknutím (případně tlačítkem *Změnit*) otevřeme dialog pro nastavení parametrů VPN serveru. V záložce *Obecné* zapneme volbu *Povolit VPN server*.

   Poznámka: V položkách *VPN subsíť* a *Maska* je nyní uvedena automaticky vybraná volná subsíť pro VPN. Nastavenou subsíť není třeba měnit.

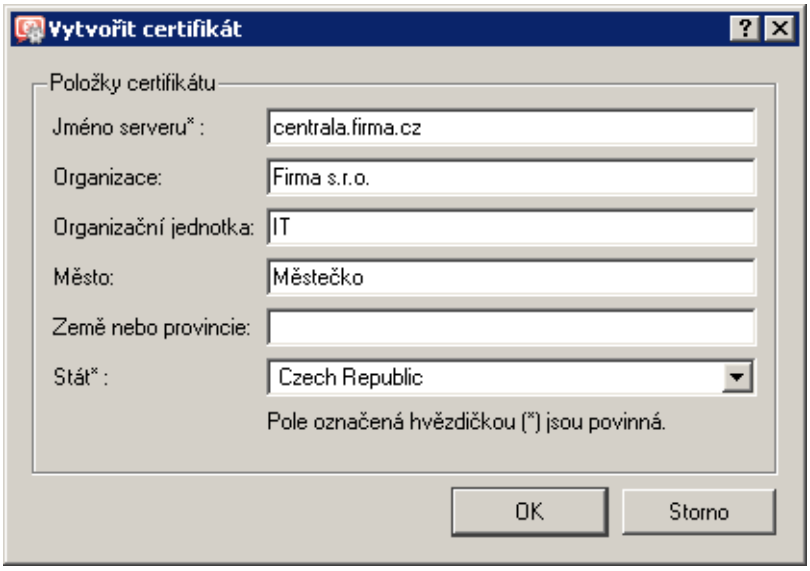


Obrázek 4.2 Centrála — konfigurace VPN serveru

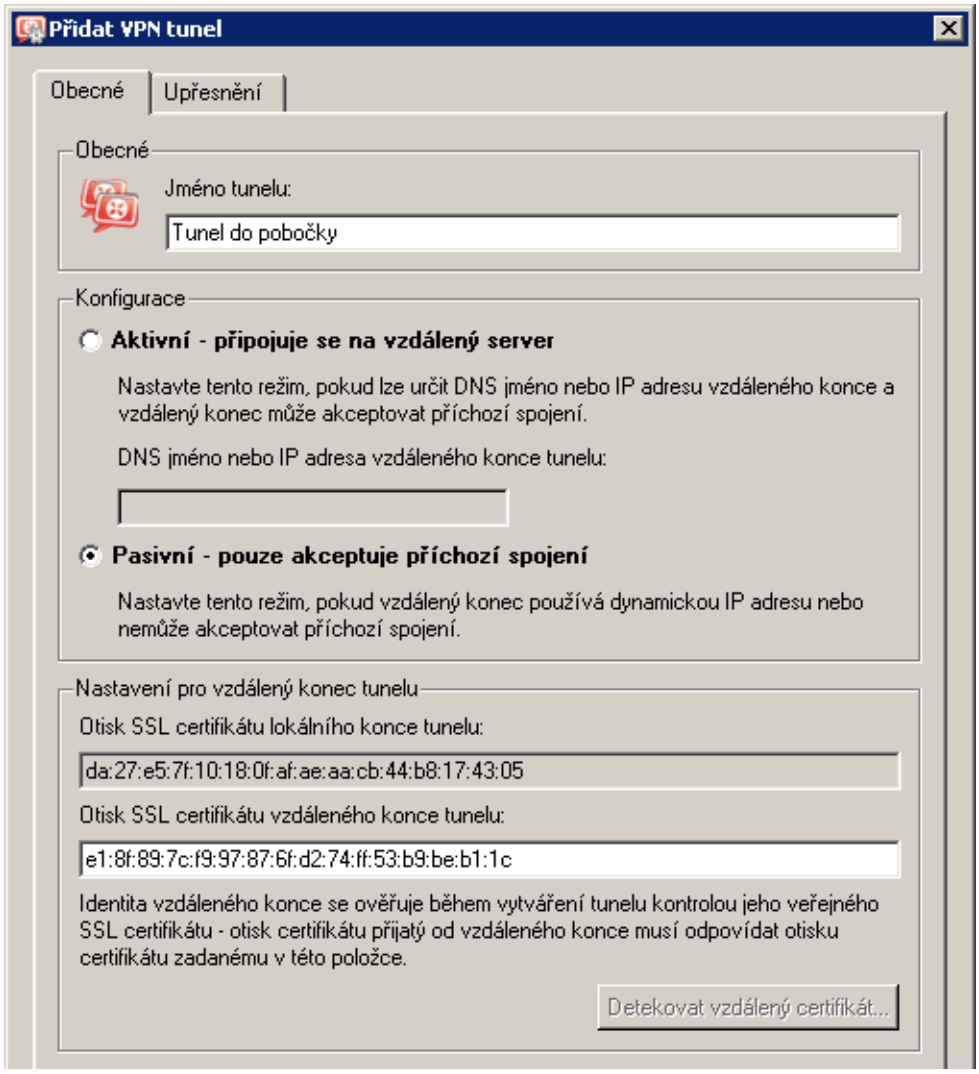
   Stiskneme tlačítko *Změnit SSL certifikát*. Pomocí tlačítka *Vytvořit certifikát* vytvoříme SSL certifikát VPN serveru (slouží pro ověření identity serveru).

   Poznámka: Vytvořený certifikát doporučujeme v budoucnu nahradit plnohodnotným certifikátem vystaveným důvěryhodnou veřejnou certifikační autoritou.

2. Vytvoříme pasivní konec VPN tunelu (server pobočky má dynamickou IP adresu). Jako otisk vzdáleného SSL certifikátu zadáme otisk certifikátu VPN serveru na pobočce.



Obrázek 4.3 Centrála — vytvoření SSL certifikátu VPN serveru



Obrázek 4.4 Centrála — pasivní konec VPN tunelu do pobočky

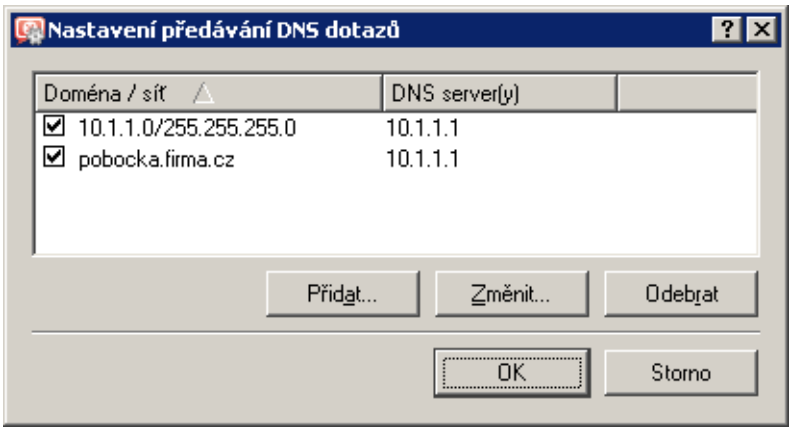
3. VPN tunel doplníme do komunikačního pravidla *Lokální komunikace* (vytvořeného *Průvodcem komunikačními pravidly* — viz kapitola 2.4).

Jméno	Zdroj	Cíl	Služba	Akce	Překlad
Služba Kerio VPN	Libovolný	Firewall	Kerio VPN	✓	
Lokální komunikace	Firewall Všichni VPN klienti Tunel do pobočky Důvěryhodné / lokální	Firewall Všichni VPN klienti Tunel do pobočky Důvěryhodné / lokální	Libovolný	✓	
Komunikace firewallu	Firewall	Libovolný	Libovolný	✓	

Obrázek 4.5 Centrála — přidání VPN tunelu do komunikačních pravidel

Poznámka: Pravidla *Komunikace firewallu* a *Služba Kerio VPN* jsou na obrázku 4.5 uvedena pro ilustraci — obě tato pravidla jsou nutná pro navázání VPN tunelu.

4. V konfiguraci *DNS Forwarderu* (viz kapitola 2.6) zapneme volbu *Použít nastavení pro předávání DNS dotazů* a definujeme pravidla pro doménu `pobocka.firma.cz`. Jako DNS server pro předávání dotazů uvedeme IP adresu vnitřního rozhraní počítače s *WinRoute* na protější straně tunelu (tj. rozhraní připojeného do lokální sítě na protější straně).



Obrázek 4.6 Centrála — konfigurace předávání DNS dotazů

4.2 Konfigurace v pobočce firmy

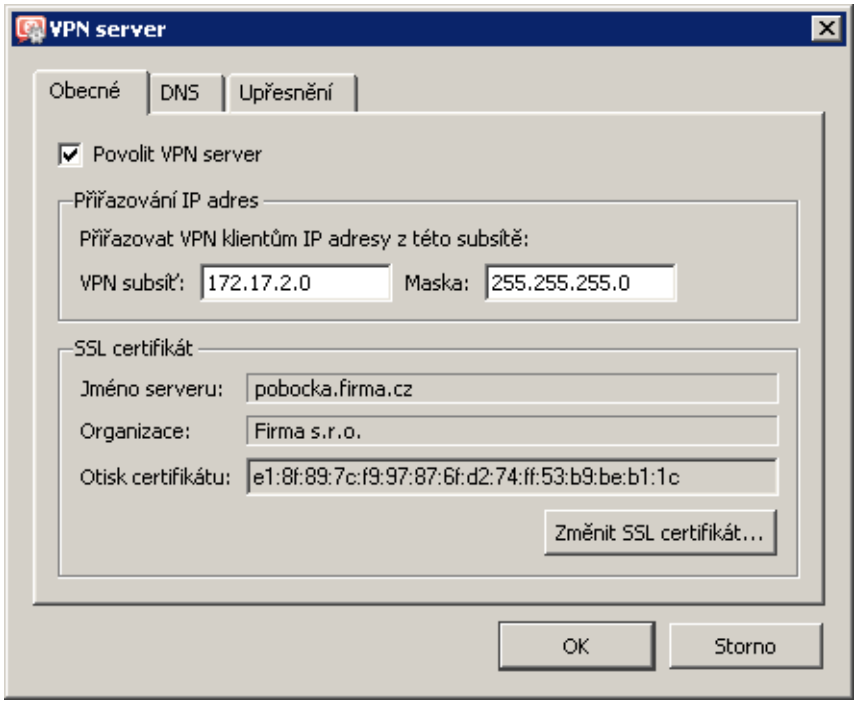
1. Ve *WinRoute* v sekci *Konfigurace / Rozhraní*, záložka *Rozhraní* vybereme *VPN server*. Dvojitým kliknutím (případně tlačítkem *Změnit*) otevřeme dialog pro nastavení parametrů VPN serveru. V záložce *Obecné* zapneme volbu *Povolit VPN server*.

   Poznámka: V položkách *VPN subsíť* a *Maska* je nyní uvedena automaticky vybraná volná subsíť pro VPN. Nastavenou subsíť není třeba měnit.

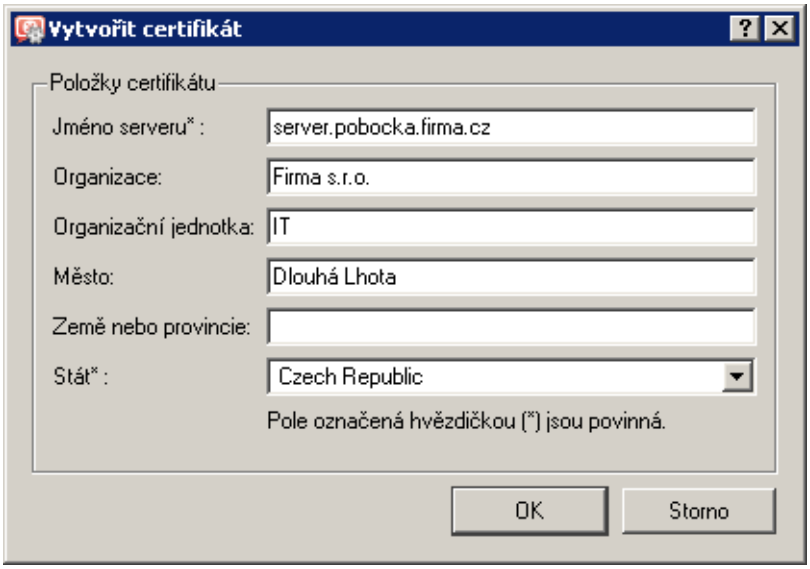
   Stiskneme tlačítko *Upřesnění* a v dialogu pro nastavení upřesňujících parametrů tlačítko *Změnit SSL certifikát*. Pomocí tlačítka *Vytvořit certifikát* vytvoříme SSL certifikát VPN serveru (slouží pro ověření identity serveru).

   Poznamenáme si otisk vytvořeného certifikátu — bude potřeba při definici VPN tunelu v centrále firmy.

   Poznámka: Vytvořený certifikát doporučujeme v budoucnu nahradit plnohodnotným certifikátem vystaveným důvěryhodnou veřejnou certifikační autoritou.



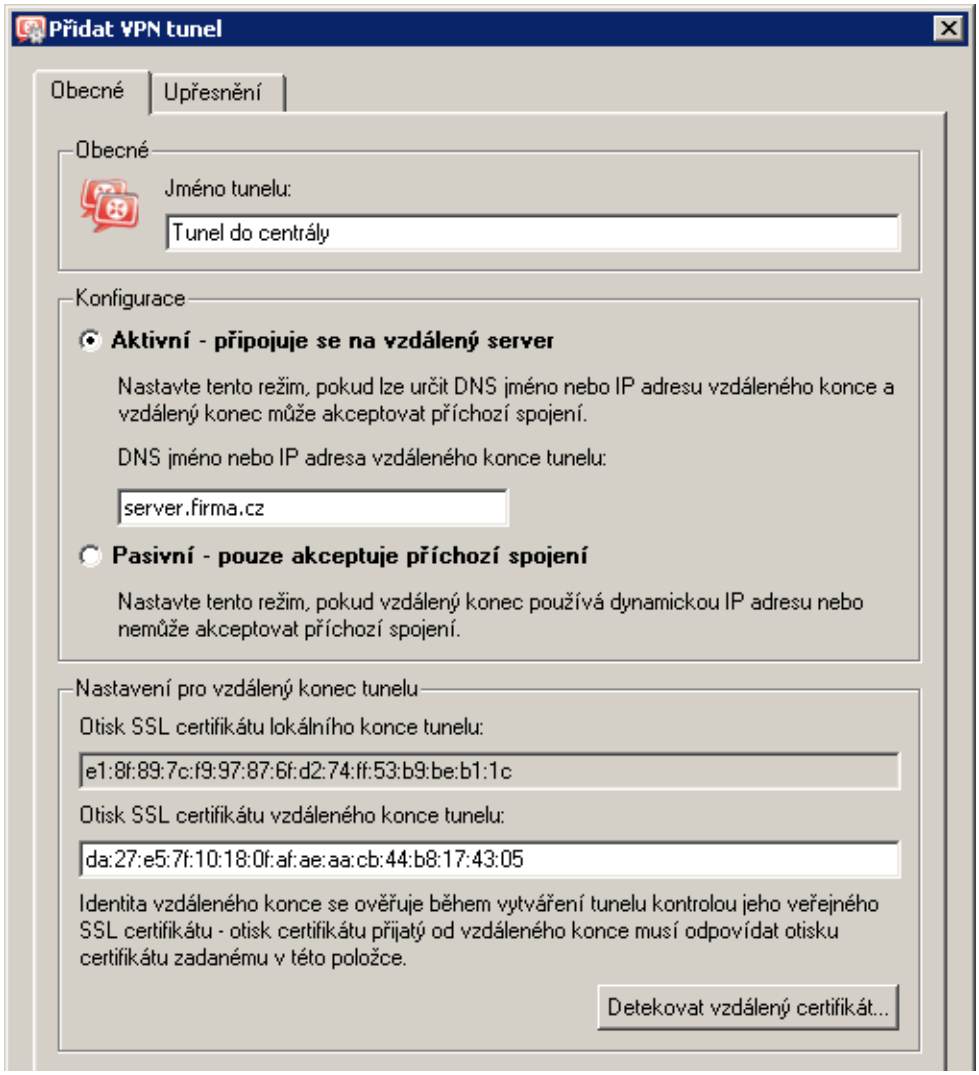
Obrázek 4.7 Pobočka — konfigurace VPN serveru



Obrázek 4.8 Pobočka — vytvoření SSL certifikátu VPN serveru

2. Vytvoříme aktivní konec VPN tunelu (server pobočky má dynamickou IP adresu). Otisk certifikátu VPN serveru v centrále firmy můžeme nastavit jednoduše stisknutím tlačítka *Detekovat vzdálený certifikát*.

3. VPN tunel doplníme do komunikačního pravidla *Lokální komunikace* (vytvořeného *Průvodcem komunikačními pravidly* — viz kapitola 2.4).



Obrázek 4.9 Pobočka — aktivní konec VPN tunelu do centrály

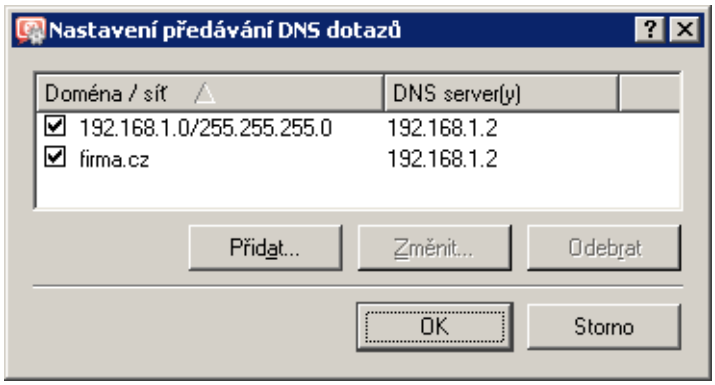
Jméno	Zdroj	Cíl	Služba	Akce	Překlad
Služba Kerio VPN	Libovolný	Firewall	Kerio VPN	✓	
Lokální komunikace	Firewall Tunel do centrály Důvěryhodné / lokální	Firewall Tunel do centrály Důvěryhodné / lokální	Libovolný	✓	
Komunikace firewallu	Firewall	Libovolný	Libovolný	✓	

Obrázek 4.10 Pobočka — přidání VPN tunelu do komunikačních pravidel

Poznámka: Pravidlo *Komunikace firewallu* je na obrázku 4.10 uvedeno pro ilustraci — toto pravidlo je nutné pro navázání VPN tunelu.

4. V konfiguraci *DNS Forwarderu* (viz kapitola 2.6) zapneme volbu *Použít nastavení pro předávání DNS dotazů* a definujeme pravidla pro doménu `firma.cz`. Jako DNS server pro pře-

dávání dotazů uvedeme IP adresu doménového serveru v centrále firmy (`192.168.1.2`), který slouží jako primární DNS server pro doménu `firma.cz`.



Obrázek 4.11 Pobočka — konfigurace předávání DNS dotazů

4.3 Test funkčnosti VPN tunelu

Po dokončení konfigurace VPN tunelu doporučujeme z každé lokální sítě vyzkoušet dostupnost počítačů v síti na protější straně tunelu.

Jako testovací nástroj lze použít např. příkazy operačního systému `ping` nebo `tracert`. Doporučujeme ověřit dostupnost počítače ve vzdálené síti zadaného jednak IP adresou, jednak DNS jménem.

Nedostaneme-li odezvu při zadání vzdáleného počítače IP adresou, je třeba hledat chybu v nastavení komunikačních pravidel, případně prověřit, zda nenastala kolize subsítí (stejná subsíť na obou stranách tunelu).

Je-li test při zadání počítače IP adresou úspěšný, ale při zadání počítače DNS jménem je hlášena chyba (*Neznámý hostitel*), pak je třeba prověřit konfiguraci DNS.

Poznámka: VPN klienti, kteří se připojují k serveru centrály, mají přístup do sítě centrály i pobočky (přístup není nijak omezen). Proto v rámci testování VPN doporučujeme vyzkoušet přístup do obou sítí také z připojeného VPN klienta.

Příloha A

Právní doložka

Microsoft®, *Windows*®, *Windows NT*® a *Active Directory*® jsou registrované ochranné známky nebo ochranné známky společnosti *Microsoft Corporation*.

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