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 *6.7*. 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.

Obsah

Kapitola 1

Úvod

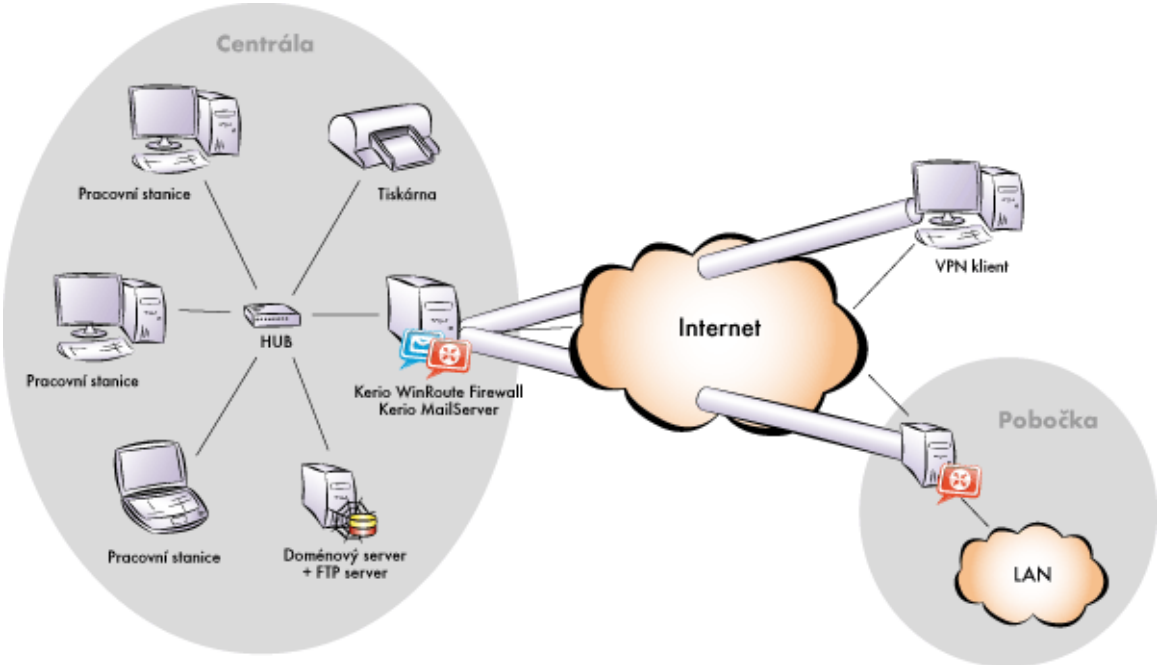
Tato příručka popisuje konfigurační úkony, které je třeba provést při nasazení aplikace *Kerio WinRoute Firewall* (dále jen *WinRoute*) v modelové síti. Uvažovaný model zohledňuje většinu požadavků, které vznikají při nasazení *WinRoute* v reálném prostředí — přístup z lokální sítě do Internetu, ochrana 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 doméně *Active Directory*, sledování statistik a aktivit uživatelů 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/cz/firewall/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 k 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`).

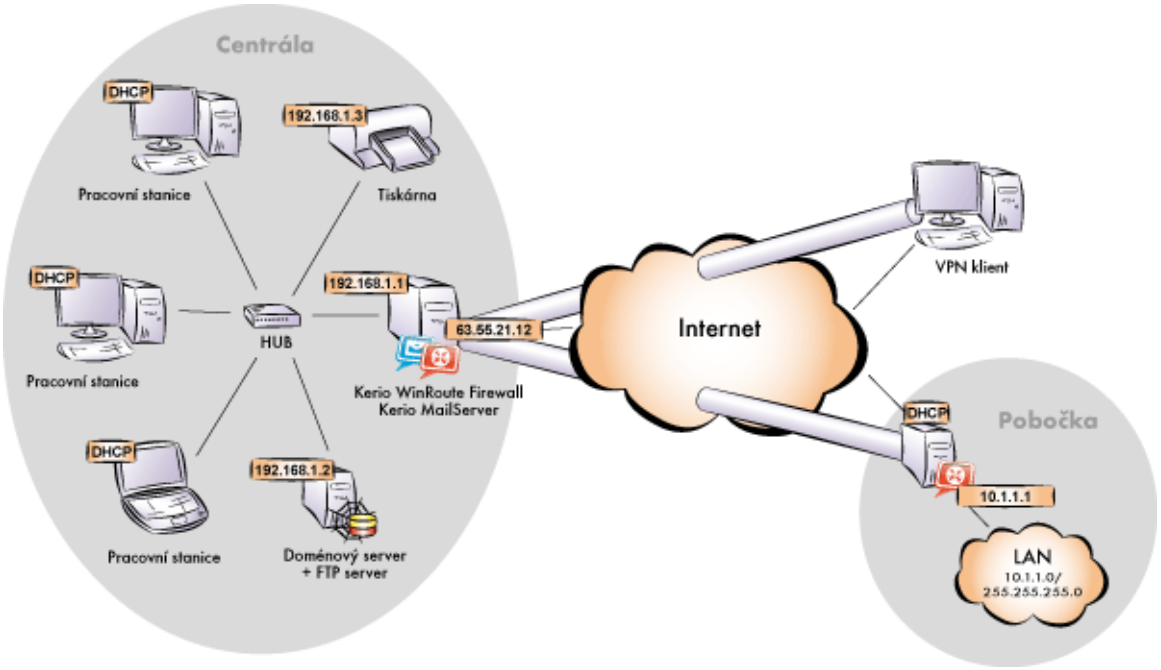
Nastavení IP adres v modelové síti

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 k Internetu

Na rozhraní připojeném k 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 k lokální síti

Na rozhraní připojeném k lokální síti 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 (IP adresa `192.168.1.2`).

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 *Sdílení připojení k Internetu* (*Internet Connection Sharing*), pak striktně doporučujeme tuto službu zakázat, jinak může docházet ke 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*.

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 (*strana 2*) — zvolíme trvalé připojení jednou internetovou linkou.
- Rozhraní připojené k Internetu (*strana 3*) — vybereme adaptér připojený k Internetu.
- Pravidla pro odchozí komunikaci (*strana 4*) — povolíme přístup z lokální sítě ke všem službám v Internetu.
- Pravidla pro VPN (*strana 5*) — ponecháme zapnuté obě volby: *Vytvořit pravidla pro Kerio VPN* (tím budou vytvořena komunikační pravidla nutná pro propojení sítí centrály a pobočky a pro připojování vzdálených klientů — viz kapitola 4) a *Vytvořit pravidla pro Kerio Clientless SSL-VPN* (vzdálený přístup ke sdíleným složkám a souborům v síti prostřednictvím WWW prohlížeče).

  Poznámka: Na firewallu 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). Proto volbu pro vytvoření pravidel pro *Clientless SSL-VPN* vypneme.
- Pravidla pro příchozí komunikaci (*Krok 6*) — přidáme mapování služby SMTP na firewallu.

  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.

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:

- *Rozsah adres* — nastavíme `192.168.1.10 - 192.168.1.254` (IP adresy `192.168.1.1 - 192.168.1.9` zůstanou vyhrazeny pro servery a tiskárny).
- *Maska subsítě* — `255.255.255.0`
- *Výchozí brána* — IP adresa rozhraní firewallu připojeného k lokální síti (`192.168.1.1`).
- *DNS server* — IP adresa rozhraní firewallu připojeného k lokální síti (`192.168.1.1` — 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 přidáme 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.

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 přehledu přidělených IP adres tuto adresu označte a stiskněte tlačítko *Rezervovat...*. Zobrazí se dialog pro rezervaci adresy, ve kterém bude již vyplněna příslušná MAC adresa. Změňte přidělenou IP adresu na požadovanou (`192.168.1.3`), případně popis, a tiskněte tlačítko *OK*. Pak tiskárnu restartujte. Po restartu přidělí DHCP server tiskárně správnou IP adresu.

Poznámky:

1. DHCP server doporučujeme zapnout (povolit) 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 připojeného k lokální síti (`192.168.1.1`).

2.6 Nastavení modulu DNS

V sekci *Konfigurace → DNS* ponecháme výchozí nastavení (povolena služba *DNS forwarder* a jednoduchý převod DNS jmen s využitím souboru `hosts` a tabulky přidělených adres DHCP serveru) a provedeme upřesňující nastavení:

- Doplníme jméno lokální DNS domény — `firma.cz`.
- 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. Toto je nutné pro správnou komunikaci počítačů v lokální síti s doménovým serverem.

DNS jméno	Předat DNS serverům
_*	192.168.1.2

Tabulka 2.1 Pravidlo pro předávání DNS dotazů do Active Directory

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

2.7 Certifikáty WWW rozhraní a SSL-VPN

WWW rozhraní *WinRoute* zajišťuje 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. Rozhraní *Clientless SSL-VPN* slouží pro zabezpečený vzdálený přístup ke sdíleným souborům v lokální síti prostřednictvím WWW prohlížeče.

Pro správnou funkci zabezpečených webových služeb je vyžadován SSL certifikát, který prokazuje totožnost serveru. Certifikáty pro webová rozhraní vytvoříme v sekci *Konfigurace → Další volby*, záložka *WWW rozhraní / SSL-VPN*. V upřesňujících nastaveních pro každé rozhraní zvolíme *Změnit SSL certifikát* a *Vytvořit certifikát*.

Jméno serveru, na které bude certifikát vystaven, by mělo být shodné se jménem serveru včetně domény detekovaným z operačního systému (viz položka *Jméno serveru, na němž WinRoute běží* — v našem příkladu `kwf.kerio.cz`). Pro přístup k webovým rozhraním *WinRoute* z Internetu musí pro toto jméno existovat záznam také ve veřejném DNS.

Tip

Vytvořené SSL certifikáty doporučujeme nahradit plnohodnotnými SSL certifikátem vystaveným některou veřejnou certifikační autoritou (pro WWW rozhraní i rozhraní *Clientless SSL-VPN* lze použít stejný certifikát — není nutné platit za dva certifikáty).

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

Ve *WinRoute* proto není třeba definovat lokální uživatelské účty, stačí mapovat příslušnou doménu. Mapování *Active Directory* domény nastavíme v sekci *Uživatelé a skupiny → Uživatelé*, záložka *Active Directory*.

Pro nastavení mapování je potřeba zadat DNS jméno domény — v našem případě `firma.cz` a přihlašovací údaje libovolného uživatele z této domény. Pro automatické ověřování uživatelů prostřednictvím *NTLM* (WWW prohlížeče, *Kerio Outlook Connector* atd.) je potřeba zadat také jméno odpovídající domény *Windows NT* (tj. `FIRMA`).

Definice šablony uživatelských účtů

V záložce *Uživatelské účty* vybereme mapovanou *Active Directory* doménu `firma.cz`. Pokud je mapování nastaveno správně, budou zde zobrazeny všechny uživatelské účty z této domény.

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*. V záložce *Práva* nastavíme odpovídající uživatelská práva.

Tip

Nechceme-li některé doménové účty používat, můžeme je ve *WinRoute* zakázat a zakázané účty skrýt. Účty budou zakázány pouze v rámci *WinRoute*, v doméně zůstanou aktivní. Účty zablokované na doménovém serveru nebudou do *WinRoute* vůbec importovány.

2.9 Skupiny IP adres a časové intervaly

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

Poznámka: Při definici první položky musíme zadat jméno (nové) skupiny, pro přidání dalších položek již stačí vybrat existující skupinu.

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

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

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).

Filtrování reklam a zákaz přístupu na stránky určitých kategorií

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

- Pravidla *Allow automatic updates for Kerio software* a *Allow automatic updates and MS Windows activation* doporučujeme ponechat zapnutá, aby fungovaly automatické aktualizace *WinRoute* a aktualizace a aktivace operačního systému serveru.

- Pravidla *Allow popular search engines* (povolit populární internetové vyhledávače) a *Remove advertisement and banners* (blokovat reklamy a bannery) můžeme použít dle uvážení.

- Pravidlo *Deny sites rated in Kerio Web Filter categories* (zakázat stránky zařazené modulem *Kerio Web Filter* do vybraných kategorií) můžeme využít k blokování přístupu na stránky s erotickým obsahem všem uživatelům.

  V definici pravidla musíme (tlačítkem *Vybrat hodnocení...*) zvolit kategorie modulu *Kerio Web Filter*, které chceme blokovat. Pro zakázání přístupu na stránky s erotickým obsahem vybereme všechny kategorie ve skupině *Pornografie / Nahota*.

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

Omezení přístupu na stránky s nabídkami zaměstnání

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

1. Přidáme pravidlo povolující skupině uživatelů *Personální oddělení* přístup na stránky kategorizované modulem *Kerio Web Filter* jako *Nabídky zaměstnání*.
2. Za toto pravidlo přidáme pravidlo zakazující přístup na tutéž kategorii stránek všem uživatelům.
   V tomto pravidle je vhodné nevyžadovat ověření uživatele. Tím zabráníme přesměrování prohlížeče uživatele na přihlašovací stránku před zobrazením informace o zákazu, pokud není uživatel dosud na firewallu ověřen.

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 příslušnou volbou v sekci *Uživatelé a skupiny → Uživatelé*, záložka *Volby pro ověřování*.

Ověření uživatele probíhá přesměrováním na přihlašovací stránku WWW rozhraní *WinRoute*. WWW rozhraní musí být povoleno a správně nastaveny jeho parametry (viz kapitola 2.7). Po zadání platného uživatelského jména a hesla dojde k přesměrování na stránku, kterou uživatel původně požadoval.

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).

Dle potřeby a s ohledem na velikost dostupného místa na disku upravíme velikost cache. Výchozí hodnota je `1 GB` (`1024 MB`), maximum je téměř `2 GB` (`2047 MB`).

2.11 Nastavení pravidel pro FTP

Požadavky

Používání FTP bude omezeno následujícím způsobem:

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

Omezení FTP s využitím předdefinovaných pravidel

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

- Pravidla *Forbid *.mpg, *.mp3 and *.mpeg* files a *Forbid upload* máme přímo k dispozici.
- Pravidlo *Forbid *.avi files* upravíme tak, že v záložce *Upřesnění* nastavíme časovou platnost v intervalu *Pracovní doba* (viz kapitola 2.9).
- Doporučujeme zapnout také pravidlo *Forbid resume due to antivirus scanning* (zakázat pokračování v přenosu souboru po přerušení z důvodu antivirové kontroly), aby mohly být všechny soubory přenášené protokolem FTP důsledně kontrolovány antivirovým programem.

FTP server v lokální síti

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:

- V záložce *Obecné* nastavíme: „pokud libovolný uživatel přistupuje na FTP server `192.168.1.10`, pak povolit.“
- V záložce *Upřesnění* upřesníme, že se jedná o typ operace *Upload* a libovolný soubor (*).

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. Tímto způsobem lze také povolit 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, nejprve jej nainstalujeme. Antivirový program *McAfee* je součástí *WinRoute* a pro jeho činnost je třeba pouze speciální licence. Ideální je použít kombinaci integrovaného a externího antiviru (tzv. duální antivirová kontrola).

V sekci *Konfigurace → Filtrování obsahu → Antivirus*, záložka *Antivirový program*, nastavíme požadované antiviry, případně upřesňující volby pro vybraný externí antivirus. Kompletní seznam podporovaných antivirů a podrobné návody pro jejich nastavení naleznete na adrese http://www.kerio.cz/cz/firewall/third-party#av.

WinRoute umožňuje zvolit protokoly, na které má být antivirová kontrola implicitně aplikována. Záložky *Kontrola HTTP a FTP*, *Kontrola e-mailu* a *Kontrola SSL-VPN* 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.

Jméno	Zdroj	Cíl	Služba	Akce	Překlad
Přístup k FTP serveru	*Libovolný*	*Firewall*	*FTP*	*Povolit*	*Mapování 192.168.1.2*

Tabulka 2.2 Zpřístupnění lokálního FTP serveru z Internetu

- Přístup ke službám poštovního serveru (kromě SMTP) — povolíme pouze z požadovaných IP adres v časovém intervalu *Pracovní doba*.

Jméno	Zdroj	Cíl	Služba	Akce	Překlad	Časová platnost
Přístup k e-mailu	Skupina adres *Přístup k e-mailu*	*Firewall*	*IMAP* *IMAPS* *POP3* *POP3S*	*Povolit*		*Pracovní doba*

Tabulka 2.3 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* (podrobnosti viz kapitola 4.1). Žádná další nastavení nejsou třeba. Komunikace VPN klientů je již povolena pravidly vytvořenými průvodcem — viz kapitola 2.4.

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

Aplikace Kerio VPN Client

Pro připojení k VPN serveru ve *WinRoute* musí být na každém vzdáleném počítači nainstalována aplikace *Kerio VPN Client*. Tato aplikace je k dispozici pro platformy *Windows*, *Mac OS X* a *Linux*. Instalační soubory lze stáhnout z WWW stránky `http://www.kerio.cz/cz/firewall/download`.

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 svým doménovým uživatelským jménem a heslem (viz kapitola 2.8).

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

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`).

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

2.16 Sledování statistik využívání Internetu a aktivit uživatelů

WinRoute nabízí webové rozhraní *Kerio StaR* (*statistiky a reportování*), které umožňuje zobrazit aktivity uživatelů a statistické informace v podobě tabulek a grafů.

Mezi sledované aktivity jednotlivých uživatelů patří:

- navštívené WWW stránky,
- e-mailové zprávy a instant messaging (zasílání rychlých zpráv),
- přenosy velkých souborů,
- multimédia (online přehrávání zvuku a videa),
- vzdálený přístup (terminálový přístup a VPN připojení).

Ve formě tabulek a grafů lze zobrazit tyto statistické informace:

- objem přenesených dat,
- používané protokoly (služby),
- nejnavštěvovanější webové domény,
- nejnavštěvovanější kategorie WWW stránek.

Statistiky lze zobrazit celkově nebo pro jednotlivé uživatele.

Přístup a přihlášení ke statistikám

Statistiky využívání Internetu mohou obsahovat citlivé informace. Z tohoto důvodu je přístup ke statistikám řízen speciálním právem, které má ve výchozím nastavení pouze uživatel *Admin*. Proto je nejprve potřeba ve správě firewallu v sekci *Uživatelé a skupiny* nastavit vybraným uživatelům a/nebo skupinám právo prohlížet statistiky.

Statistiky jsou dostupné prostřednictvím WWW rozhraní *WinRoute*. Do WWW rozhraní se lze přihlásit na adrese:

`https://<firewall>:4081/`

v našem příkladu tedy:

`https://kwf.firma.cz:4081/`

Uživatelům s právem prohlížet statistiky se po přihlášení do WWW rozhraní zobrazí přímo stránka *Kerio StaR* s celkovými statistikami. *Kerio StaR*. Ostatním uživatelům se zobrazí úvodní stránka WWW rozhraní.

WWW rozhraní je standardně dostupné z lokální sítě. Pro zpřístupnění tohoto rozhraní z Internetu je potřeba nastavit odpovídající komunikační pravidlo (viz kapitola 2.13).

Bližší informace o WWW rozhraní *WinRoute* a o *Kerio StaR* naleznete v manuálu *Kerio WinRoute Firewall — Příručka uživatele*, který je k dispozici na WWW stránce http://www.kerio.cz/cz/firewall/manual.

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. Rozdíly jsou pouze v konfiguraci DNS a DHCP. Předpokládejme, že v síti pobočky firmy není doménový server ani žádný jiný DNS server. Funkci primárního DNS serveru zde bude plnit modul *DNS* ve *WinRoute*.

3.1 Konfigurace síťových rozhraní internetové brány

Na rozhraní firewallu připojeném k lokální síti 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!

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

3.2 Nastavení modulu DNS

V sekci *Konfigurace → DNS* ponecháme výchozí nastavení (povolena služba *DNS forwarder* a jednoduchý převod DNS jmen s využitím souboru `hosts` a tabulky přidělených adres DHCP serveru) a provedeme upřesňující nastavení:

- Doplníme jméno lokální DNS domény — `pobocka.firma.cz`.
- Zapneme volbu *Použít nastavení pro předávání DNS dotazů*. Toto nastavení bude podrobně popsáno v kapitole 4.2.
- Do souboru *hosts* je vhodné přidat záznam o serveru (případně o dalších počítačích, kterým bude nastavena pevná IP adresa):
  `10.1.1.1 server`

3.3 Nastavení DHCP serveru

V sekci *Konfigurace → DHCP server* vytvoříme rozsah adres dynamicky přidělovaných pracovním stanicím (volba *Přidat → Rozsah adres...*). Při definici rozsahu je třeba specifikovat tyto parametry:

- *Rozsah adres* — nastavíme `10.1.1.10 - 10.1.1.254` (IP adresy `10.1.1.1 - 10.1.1.9` zůstanou vyhrazeny pro servery a tiskárny).
- *Maska subsítě* — `255.255.255.0`
- *Výchozí brána* — IP adresa rozhraní firewallu připojeného k lokální síti (`10.1.1.1`).
- *DNS server* — IP adresa rozhraní firewallu připojeného k lokální síti (`10.1.1.1` — 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.

Kapitola 4

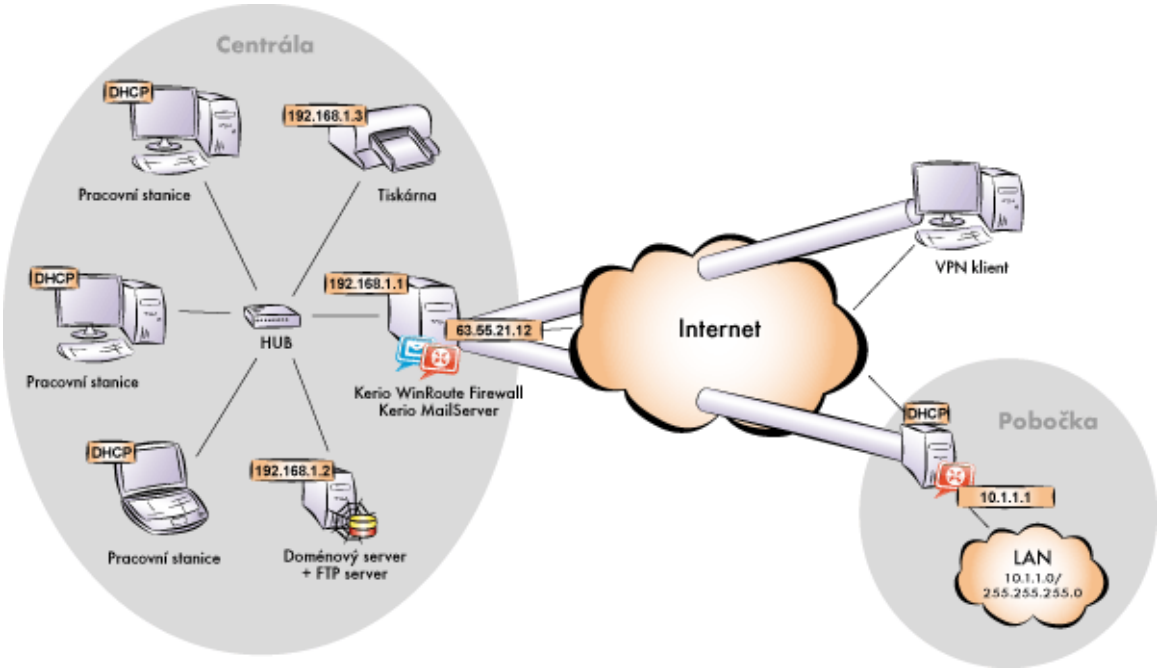
Propojení sítí centrály a pobočky

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* vybereme *VPN server*, otevřeme dialog pro nastavení jeho parametrů a povolíme jej.
   Poznámka: V položkách *VPN subsíť* a *Maska* je nyní uvedena automaticky vybraná volná subsíť pro VPN. Nastavenou subsíť není třeba měnit.
   Tlačítkem *Změnit SSL certifikát* vytvoříme SSL certifikát se jménem příslušného serveru (např. `kwf.firma.cz`). Tento certifikát slouží pro ověření identity VPN 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 — na pobočce proto musí být aktivní konec tunelu). Jako otisk SSL certifikátu vzdáleného konce tunelu zadáme otisk certifikátu VPN serveru na pobočce.
3. VPN tunel doplníme do komunikačního pravidla *Lokální komunikace* (vytvořeného *Průvodcem komunikačními pravidly* — viz kapitola 2.4).

Jméno	Zdroj	Cíl	Služba	Akce	Překlad
Lokální komunikace	*Firewall* *Všichni VPN klienti* *Tunel do pobočky* *Důvěryhodné* */ lokální*	*Firewall* *Všichni VPN klienti* *Tunel do pobočky* *Důvěryhodné* */ lokální*	*Libovolná*	*Povolit*	

Tabulka 4.1 Centrála — komunikační pravidlo Lokální komunikace

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 k lokální síti na protější straně).

Doména / síť	DNS server(y)
`10.1.1.0 / 255.255.255.0`	`10.1.1.1`
`pobocka.firma.cz`	`10.1.1.1`

Tabulka 4.2 Centrála — konfigurace předávání DNS dotazů

4.2 Konfigurace v pobočce firmy

1. Ve *WinRoute* v sekci *Konfigurace / Rozhraní* vybereme *VPN server*, otevřeme dialog pro nastavení jeho parametrů a povolíme jej.
   Poznámka: V položkách *VPN subsíť* a *Maska* je nyní uvedena automaticky vybraná volná subsíť pro VPN. Nastavenou subsíť není třeba měnit.
   Tlačítkem *Změnit SSL certifikát* vytvoříme SSL certifikát se jménem příslušného serveru (např. `server.pobocka.firma.cz`). Tento certifikát slouží pro ověření identity VPN ser-

veru. Otisk vytvořeného SSL certifikátu budeme potřebovat při definici VPN tunelu na serveru centrály (viz kapitola 4.1). Proto jej označíme, zkopírujeme do schránky a vložíme do e-mailové zprávy, souboru apod.
Poznámka: Vytvořený certifikát doporučujeme v budoucnu nahradit plnohodnotným certifikátem vystaveným důvěryhodnou veřejnou certifikační autoritou.

2. Vytvoříme *aktivní* konec VPN tunelu, který se připojuje na server centrály firmy (`kwf.firma.cz`). Otisk SSL certifikátu VPN serveru v centrále 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).

Jméno	Zdroj	Cíl	Služba	Akce	Překlad
Lokální komunikace	*Firewall* *Tunel do pobočky* *Důvěryhodné* */ lokální*	*Firewall* *Tunel do pobočky* *Důvěryhodné* */ lokální*	*Libovolná*	*Povolit*	

Tabulka 4.3 Pobočka — komunikační pravidlo Lokální komunikace

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

Doména / síť	DNS server(y)
`192.168.1.0 / 255.255.255.0`	`192.168.1.2`
`firma.cz`	`192.168.1.2`

Tabulka 4.4 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