



Konfigurace a provoz verze 4.5

Cílem tohoto dokumentu je stručnou a přehlednou formou Vás seznámit s postupem instalace a konfigurace nové verze Mail602 Messaging Serveru včetně zprovoznění různých druhů klientských přístupů k poštovnímu úřadu.

Mail602 MESSAGING SERVER 4.5

Komplexní komunikační systém přinášející bezpečné internetové služby a poštu pro celou Vaši síť, dále faxování, odesílání SMS zpráv, hlasový záznamník pro každého uživatele a navíc možnost použití téměř libovolného klientského programu.

Jádro celého systému tvoří poštovní úřad, na kterém se nacházejí zásilky a ke kterému uživatelé přistupují klientskými programy z lokální sítě a prostřednictvím komunikačního serveru i odkudkoliv z Internetu. Pro přístup k poště lze používat browser (např. Internet Explorer), POP3 klienta (např. Outlook Express), MAPI klienta (např. Outlook 9x/2000), program Mail602 Klient a nebo mobilní telefon s podporou WAP.

Mezi hlavní rysy celého systému patří bezpečnost. **Firewall** chrání server i síť proti útokům a neoprávněným pokusům o průnik z internetu (pouze na Windows 2000/2003/XP). K vyšší bezpečnosti přispívá také **podpora elektronického podpisu, šifrování obsahu zásilek i datových přenosů**. O efektivní a bezpečné využívání elektronické pošty se stará vestavěný **antivirový systém BitDefender™** a server má implementováno i rozhraní pro spolupráci se systémem AVG. Neznámé viry a zbytečné soubory pomáhá odstranit **filtr nebezpečných příloh**, zatímco nevyžádané zásilky blokuje **inteligentní antispam**.

Pro usnadnění administrace je k dispozici kompletní **dálková konfigurace a správa** prostřednictvím webu a technologie DCOM. **Uživatele lze asociovat se síťovým OS** (Novell NDS&Bindery a MS Windows NT/2000/XP) a přímo jim tak nastavit potřebná práva.

Obsah

| | |
|--|-----------|
| MAIL602 MESSAGING SERVER 4.5 | 1 |
| OBSAH | 2 |
| INSTALACE ADMINISTRÁTORA A MESSAGING SERVERU | 4 |
| DŮLEŽITÉ POZNÁMKY K INSTALACI | 4 |
| UPGRADE Z VERZE 4.0/4.1 | 6 |
| KONFIGURACE | 7 |
| REGISTRACE A LICENCOVÁNÍ | 7 |
| ZALOŽENÍ (PŘIDÁNÍ) UŽIVATELŮ | 7 |
| NASTAVENÍ ARCHIVACE ZÁSILEK | 8 |
| NASTAVENÍ KÓDOVÁNÍ ZÁSILEK | 9 |
| PRVNÍ SPUŠTĚNÍ MESSAGING SERVERU | 9 |
| VOLBA ZPŮSOBU PŘIPOJENÍ K INTERNETU | 9 |
| ZABEZPEČENÍ POMOCÍ FIREWALLU..... | 10 |
| KONFIGURACE ODESÍLÁNÍ A PŘÍJMU E-MAILŮ (NASTAVENÍ SMTP)..... | 12 |
| KONFIGURACE PŘÍJMU E-MAILŮ (NASTAVENÍ POP3)..... | 18 |
| ANTIVIROVÁ KONTROLA ZÁSILEK | 21 |
| FILTRACE PŘÍLOH..... | 22 |
| ANTISPAM..... | 24 |
| PŘÍSTUP NA INTERNET POMOCÍ PŘEKladu ADRES (NAT) | 27 |
| KONFIGURACE SDÍLENÉHO PŘÍSTUPU K INTERNETU (PROXY)..... | 29 |
| KONFIGURACE WWW SERVERU | 35 |
| KONFIGURACE FAXOVÁNÍ (NASTAVENÍ SLUŽBY FAX)..... | 37 |
| KONFIGURACE TELEFONNÍHO ZÁZNAMNÍKU | 38 |
| ZPŘÍSTUPNĚNÍ INFORMACÍ O UŽIVATELÍCH (NASTAVENÍ LDAP)..... | 40 |
| KONFIGURACE ODESÍLÁNÍ A PŘÍJMU SMS..... | 40 |
| KONFIGURACE SPOJENÍ MAIL602..... | 40 |
| KONFIGURACE NT/2000 SLUŽBY | 43 |
| VZDÁLENÁ SPRÁVA | 44 |
| KLIENSKÉ PROGRAMY | 47 |
| NASTAVENÍ INTERNETOVÉHO PROHLÍZEČE | 47 |
| ELEKTRONICKÝ PODPIS A ŠIFROVÁNÍ ZÁSILEK (S-MIME) | 48 |
| MAIL602 KLIENT | 50 |
| OVLÁDÁNÍ PROGRAMU MAIL602 KLIENT | 51 |

| | |
|---|-----------|
| POP3 KLIENT | 53 |
| OBECNÝ SMTP/POP3 POŠTOVNÍ KLIENT | 54 |
| OUTLOOK EXPRESS | 54 |
| JAK FAXOVAT Z POP3 KLIENTA ? | 55 |
| NASTAVENÍ OUTLOOK EXPRESS PRO SSL SMTP/POP3 | 56 |
| VYHLEDÁVÁNÍ E-MAILOVÝCH ADRES A INFORMACÍ U UŽIVATELÍCH | 57 |
| MAPI KLIENT (MS OUTLOOK 9X/2000) | 57 |
| INSTALACE MAPI PODPORY | 58 |
| PŘÍSTUP K POŠTĚ A NASTAVENÍM SYSTÉMU MAIL602 | 58 |
| POZNÁMKY | 58 |
| WWW KLIENT | 58 |
| WAP KLIENT | 59 |
| SYSTÉMOVÉ POŽADAVKY | 60 |

Instalace Administrátora a Messaging Serveru

Mail602 Messaging Server je vhodné instalovat na počítač s faxmodemem (či obdobným zařízením), připojený k Internetu a splňující příslušné systémové požadavky.

- 0) Připravte si k ruce licenční číslo serveru (M45-...). Pokud ho ještě nemáte, můžete jej ZDARMA získat na stránce <http://www.602.cz/registrace/msg45.htm>
- 1) Po spuštění instalace Mail602 Messaging Serveru (stažený soubor, z úvodní obrazovky nebo z adresáře MESSAG\SERVER\Disk1 na CD) zvolte cílový adresář a při výběru komponent zaškrtněte instalaci Administrátora i Messaging Serveru.
- 2) V dotazu týkajícím se napojení na již existující poštovní úřad ponechte řádku prázdnou. Pouze pokud provádíte upgrade nebo chcete server provozovat nad již existujícím poštovním úřadem, zadejte zde cestu na soubor M602.EMI.
- 3) Pokud jste se při instalaci nenapojili na existující poštovní úřad, pak po instalaci potvrďte nabízené spuštění průvodce konfigurací nového poštovního úřadu a postupujte podle jeho pokynů.
- 4) Zadejte licenční číslo serveru a zvolte cestu pro založení poštovního úřadu. Poštovní úřad je vhodné založit na sdíleném diskovém prostoru, přičemž cestu lze zapsat i v UNC formátu ([\\počítač\sdílení\cesta](#)).
- 5) Po zadání názvu poštovního úřadu (max. 8 znaků) věnujte ZVÝŠENOU POZORNOST zadání kódovacího řetězce i hesla SUPERVISORA! Pro jistotu si oba tyto údaje ihned zaznamenejte a uschovejte na bezpečné místo, neboť jsou nutné pro následné provádění změn v konfiguraci.
- 6) V posledním kroku zadejte internetovou doménu (např. firma.isp.cz), kterou máte zaregistrovanou u svého poskytovatele připojení.

Důležité poznámky k instalaci

Předpoklady pro asociaci uživatelů

Asociace uživatelů tj. jejich on-line provázání s operačním systémem lze využívat v následujících případech:

- poštovní úřad je založen na disku počítače s Windows NT/2000/XP/2003,
- poštovní úřad je založen na disku serveru Novell Netware v režimu Bindery,
- na síti je k dispozici Novell NDS a stanice pro přístup do sítě využívají síťového klienta od firmy Novell.

Díky asociacím jednoduše převezmeme uživatele ze síťového operačního systému do systému Mail602. Následně můžete asociovaným uživatelům nastavit potřebná síťová práva stisknutím jednoho tlačítka. Uživatel se pak také hlásí pouze do sítě (jméno a heslo) a přihlášení do pošty je ze sítě automaticky převzato – platí pouze pro přístup pomocí Mail602 Klient a Microsoft Outlook 9x/2000. Při přístupu k poště jiným způsobem (POP3, WEB, WAP) se používá shodné přihlašovací jméno a heslo jako do sítě.

Předpoklady pro vzdálenou správu poštovního úřadu – DCOM

Pokud budete chtít využívat vzdálenou správu poštovního úřadu prostřednictvím technologie DCOM (protokolem TCP/IP např. z Internetu, tzn. nejen klasicky po lokální síti prostřednictvím sdílení poštovního adresáře), nainstalujte program Administrátor (také) na počítač s operačním systémem Windows NT/2000/XP (tzv. *administrační server*), ze kterého je po síti dostupný poštovní úřad. Administrační server musí být dostupný protokolem TCP/IP z lokality, ze které chcete poštovní úřad spravovat (např. z Internetu).

Na tomto administračním serveru je dále třeba založit uživatele se shodným jménem a heslem jako bude na vzdáleném počítači používat vzdálený správce a přidat ho ve Windows do skupiny Administrátoři.

Používání pouze POP3 přístupu

V Administrátorovi je třeba alespoň jednomu z uživatelů v jeho vlastnostech na kartě „Adresy a čísla“ nastavit do přesměrování faxů podle ID řetězce znak * (hvězdička). Tomuto uživateli pak budou doručovány všechny příchozí faxy.

Pro zprávu nezařazené pošty (např. zásilek se správnou doménou ale chybnou částí adresy před zavináčem, které nebyly nikomu doručeny, ale nebyly ani odmítnuty) lze použít pouze program Mail602 Klient.

Upgrade z verze 4.0/4.1

Před započítím upgrade doporučujeme provést zálohu poštovního úřadu i složky s nainstalovanou verzí 4.0/4.1.

Neprovádějte také upgrade, pokud nemáte k dispozici distribuční nebo licenční čísla pro verzi 4.5!

- 1) Ještě před zahájením instalace doporučujeme spustit původní program Administrátor. Po přihlášení k úřadu klikněte na Registrace Messaging Serveru a zkopírujte si nebo opište původní licenční číslo serveru (M40-...).
- 2) Připravte si k ruce nové licenční číslo serveru (M45-...). Pokud ho ještě nemáte, můžete jej ZDARMA získat na stránce <http://www.602.cz/registrace/msg45.htm>
- 3) Nyní na stránce <http://www.602.cz/registrace/msg45upg.htm> proveďte aktivaci distribučního čísla pro upgrade (DMU-...). Po provedení aktivace obdržíte e-mail s licenčním číslem pro stejný počet add-on licencí, jaký jste využívali ve verzi 4.0/4.1.
- 4) Pokud máte k dispozici distribuční číslo pro add-on licence začínající DMK-..., popř. distribuční číslo pro antivirový systém BitDefender™ začínající DMB-..., aktivujte ho na stránce <http://www.602.cz/registrace/msg45lic.htm>
- 5) Nainstalujte verzi 4.5 a v závěru instalace zvolte napojení na existující poštovní úřad.
- 6) Spustíte program Administrátor a po přihlášení klikněte na Registrace Messaging Serveru a stiskněte tlačítko **Upgrade na verzi 4.5**. Zadejte licenční číslo nového serveru (M45-...).
- 7) Klikněte opět na Registrace Messaging Serveru a zadejte licenční číslo pro add-on licence (ML4-...), popř. pro antivirus (MBD-...).
- 8) Tím je upgrade hotov. Nyní můžete spustit Messaging Server verze 4.5 a začít konfigurovat nové funkce.

Konfigurace

Obecně lze konfiguraci systému Mail602 po instalaci shrnout do následujících bodů :

1. nastavení Administrátora – registrace, uživatelé, práva, ...,
2. nastavení komunikačního serveru,
3. instalace a konfigurace klientských programů.

Pokud bude v některém tématu uveden podnadpis „Administrátor“ nebo „Messaging Server“, znamená to, že popisované nastavení se provádí v příslušném programu.

Registrace a licencování

- a) Jestliže si chcete vše nejprve v klidu vyzkoušet, můžete systém Mail602 provozovat po dobu 30 dnů jako plně funkční TRIAL verzi pro 5 uživatelů.
- b) Pokud jste již rozhodnutí, můžete si licence pro daný počet uživatelů zakoupit přes stránku http://www.602.cz/produkty/kosik/kos_mess.htm
- c) Pokud jste již nakoupili, připravte si k ruce licenční čísla pro Add-on licence. Pokud máte k dispozici pouze distribuční čísla (začínají DMK-...), uplatněte je pro získání licenčních čísel zadáním do příslušných řádek na stránce <http://www.602.cz/registrace/msg45lic.htm>
Na stejné stránce se aktivuje i distribuční číslo pro antivirový systém BitDefender™ (začíná DMB-...).

Administrátor

Po spuštění Administrátora kliknutím na název poštovního úřadu zobrazte přihlašovací dialog. V některých případech může být také zapotřebí nejprve kliknout na Seznam úřadů.

Pokud chcete zadat zakoupená licenční čísla – zvýšit počet uživatelů (poštovních schránek) zadáním add-on licencí nebo zprovoznit antivirový systém BitDefender™ – vyberte položku „Registrace Messaging Serveru“ v pravé části okna s hlavní konfigurací poštovního úřadu.

Založení (přidání) uživatelů

Administrátor

Po spuštění Administrátora kliknutím na název poštovního úřadu zobrazte přihlašovací dialog. V některých případech může být také zapotřebí nejprve kliknout na Seznam úřadů.

Rozbalte strom Uživatelé a přejděte na položku Základní informace. V pravé části okna klikněte pravým tlačítkem a přidejte uživatele.

Asociace uživatele

Pokud splňuje Vaše instalace potřebné předpoklady (viz Důležité poznámky k instalaci), můžete uživatele do systému Mail602 převzít a aktivně propojit přímo se síťovým operačním systémem.

Nejprve je však třeba asociace povolit. Klikněte na název Vašeho úřadu a v pravé části okna vyberte Typ asociace uživatelů. V nastavení si vyberte z možností nabízených dle Vaší konfigurace.

Pokud tedy máte asociování uživatelů povoleno, bude Vám nabídnuto přidání a asociování uživatele ze síťového operačního systému. Po potvrzení se zobrazí seznam uživatelů síťového operačního systému, ze kterých si můžete příslušného vybrat.

Ostatní případy (neasociovaný uživatel)

Pokud Vám není asociace nabídnuta nebo zvolíte-li neasociovat, vyplňte přihlašovací a plné jméno uživatele a dvakrát heslo (lze také provést „statický“ import ze serveru).

Nastavení archivace zásilek

Administrátor

Všechny zásilky na poštovním úřadu systému Mail602 mohou být archivovány v centrálním kódovaném a komprimovaném archivu.

Nastavení parametrů archivace lze provádět v pravé části okna po kliknutí na název poštovního úřadu. Pro příchozí i odchozí zásilky lze odděleně nastavit způsob jejich archivace. U zásilek lze buď pouze evidovat jejich průvodku (tzn. bez obsahu dopisu) nebo archivovat obsah dopisu, případně i s připojenými soubory.

Odděleně se provádí nastavení pro odchozí faxy, neboť jejich grafická podoba klade zvýšené nároky na místo na disku s archivem.

Nastavení kódování zásilek

Administrátor

Všechny zásilky uložené na poštovním úřadu jsou kódovány nastavenou metodou (Standard, DES, 2*DES). Obvykle postačuje použití Standardní metody, která je i nejrychlejší.

Kódovány mohou být i faxy nacházející se ve frontě zásilek k odeslání. Doporučujeme používat volbu „nekódovat“, neboť faxy ve frontě nejsou ani při tomto nastavení běžnými prostředky čitelné. Kódování navíc zbytečně zatěžuje komunikační server.

První spuštění Messaging Serveru

Pokud server nalezne na počítači nainstalovanou předchozí verzi Messaging Serveru resp. Internet Serveru, budete při jeho prvním spuštění dotázáni, zda se má provést import „internetové“ konfigurace (SMTP, POP3, Proxy, WWW, atd.). Jestliže jste při instalaci nového Messaging Serveru napojili na stávající poštovní úřad, bude také automaticky načtena konfigurace Intranet Serveru (fax, hlas, atd.).

V ostatních případech budete muset komunikační služby nakonfigurovat ručně. Základní internetové služby lze nastavit snadno pomocí průvodce konfigurací. Čtěte pozorně všechny zobrazované informace.

Pozn. Po spuštění můžete být vyzváni k zadání cesty na poštovní úřad – vyplňte cestu, kterou jste zvolili při zakládání poštovního úřadu. Pokud po Vás server při každém spuštění vyžaduje potvrzení této cesty, můžete upravit zástupce programu Messaging Server tak, že v řádku Cíl přepíšete cestu v parametru /EMI:... tak, aby směřovala na Váš poštovní úřad.

Volba způsobu připojení k Internetu

Messaging Server

Pokud jste k Internetu připojeni pomocí modemu vytáčenou linkou nebo máte trvalé připojení realizováno jako permanentní dial-up pomocí modemů, přidejte v konfiguraci Messaging Serveru službu DIAL-UP a vyplňte jméno a heslo. Dále můžete na kartě Kdy navazovat spojení omezit časově a věcně události a intervaly, kdy je připojení navazováno.

V případě používání jediného faxmodemu pro připojení k Internetu i faxování je vhodné zapnout poslední možnost „Uvolnit TAPI zařízení ...“, která zajistí odeslání čekajících faxů.

Pro pevnou linku či jinak realizované trvalé připojení není třeba provádět žádné nastavení – Messaging Server se o navazování připojení prostě nebude starat.

Zabezpečení pomocí firewallu

Charakteristika firewallu

Firewall chrání počítač s Messaging Serverem a celou lokální síť před neoprávněnými spojeními a průniky. **Firewall je přístupný, pouze pokud je Messaging Server provozován na Windows 2000/2003 nebo XP.** Konfigurace firewallu předpokládá existenci alespoň dvou síťových rozhraní:

- vnějšího pro připojení k internetu (modem, síťová karta k routeru apod.) a
- vnitřního pro připojení lokální sítě (obvykle síťová karta).

Firewall pracuje na principu paketového filtru a nastavuje se pomocí sad povolení spojení na jednotlivých síťových rozhraních. **Pokud tedy není nějaké spojení v nastavení firewallu explicitně povoleno, je zakázáno.**

Upozornění

Nevhodným nastavením pravidel práce firewallu lze znepřístupnit ostatní komunikační služby programu Messaging Server nebo jiné síťové služby (např. sdílení)!

Konfigurace firewallu

V konfiguraci pro odborníky vyberte/přidejte FIREWALL službu. Firewall lze globálně zapnout či vypnout zaškrtnutím u této služby. I v případě, že je služba zaškrtnuta, je firewall aktivní pouze, pokud je spuštěn Messaging Server (buď jako aplikace nebo jako služba).

Pro správnou funkci většiny sad povolení je nutné nejdříve ve vlastnostech definovat, které ze síťových rozhraní je lokální = určeno pro spojení s vnitřní sítí. Ostatní rozhraní se pak považují za spojení do internetu.

Při konfiguraci firewallu lze použít buď zjednodušené rozhraní a pomocí táhla nastavit určitou úroveň bezpečnosti (**Vysoká, Střední, Nízká**) nebo pravidla pro práci firewallu zadat manuálně pomocí předdefinovaných a/nebo vlastních sad povolení (při úrovni bezpečnosti **Vlastní**).

Vlastnosti zmíněných bezpečnostních úrovní jsou popsány přímo v konfigurační kartě firewallu. Při vytváření vlastních sad povolení lze vytvářet vlastní povolení pomocí jednotlivých protokolů, směrů spojení, síťových rozhraní nebo IP adres a portů.

Nastavení vlastní úrovně bezpečnosti

Při nastavování vlastní úrovně bezpečnosti a zejména vlastních sad povolení je třeba vycházet z dobré znalosti vlastností IP spojení.

Při nastavení **Bezpečnosti** do polohy **Vlastní** se volí a upravují tzv. sady povolení. V pravé části karty je seznam aktuálních sad povolení. Tlačítka **Přidat sadu**, **Kopírovat sadu**, **Editovat sadu** a **Vymazat sadu** můžeme sady povolení přidávat, vytvářet jejich kopie pro další editaci, stávající sady editovat a sady mazat. Odškrtnutím čtverce u zvolené sady povolení je možné tuto sadu dočasně vyřadit z funkce.

Vlastní úroveň bezpečnosti obsahuje standardně po instalaci několik předdefinovaných sad povolení založených na střední úrovni bezpečnosti, které umožňují provoz a přístup k většině komunikačních služeb Messaging Serveru jak z lokální sítě, tak z internetu. Pokud se kdykoli budete chtít vrátit k tomuto výchozímu nastavení, stiskněte tlačítko **Výchozí**.

Přidání sady povolení

Při přidávání sady povolení si můžeme vybrat, zda přidáváme sadu povolení předdefinovanou výrobcem (**Přidat vybrané předdefinované sady povolení**) nebo zda přidáme sadu vlastní (**Přidat novou sadu povolení**), kterou budeme dále editovat podle svých potřeb. Editovat lze i předdefinované sady, ale je třeba je následně ukládat pod novými názvy.

Předdefinované sady povolení lze přidávat i hromadně; k současnému označení více sad použijte levé tlačítko myši spolu s klávesou **Ctrl**.

Je třeba si uvědomit, že uživatelská pravidla jsou vždy povolující, tedy povolují další spojení, pokud tedy použijete jako základ své sady povolení některou sadu přednastavenou, budete stupeň bezpečnosti dalším přidáváním povolení vždy snižovat.

Příklad použití předdefinovaných sad povolení

Pokud chcete použít nastavení prostřednictvím úrovní bezpečnosti, ale potřebujete k němu přidat další povolení (např. povolit SMTP příjem při středním stupni bezpečnosti), zvolte úroveň bezpečnosti **Vlastní**, přidejte přednastavenou sadu povolení pro zvolenou úroveň bezpečnosti a k ní přidejte další sadu(y) povolení podle aktuální potřeby. Např.:

- Povolení pro střední úroveň bezpečnosti,
- Povolení SMTP spojení z internetu na tento počítač.

Přidání nové (vlastní) sady povolení

Pokud při přidávání sady povolení zvolíte **Přidat novou sadu povolení**, otevře se Vám prázdné okno pro editaci sady povolení. **Jméno sady povolení** slouží k přehlednému pojmenování vytvářené sady a bude se následně zobrazovat v přehledu sad povolení.

Sadu povolení naplníte prostřednictvím tlačítek **Přidat**, **Editovat** a **Vymazat**, kterými přidáváte nebo modifikujete jednotlivá povolení obsažená v sadě.

Přidání / editace povolení

Konkrétní povolení přidáváme tlačítky **Přidat** nebo **Editovat** vždy do právě editované sady, která je určena svým jménem. Povolení se může týkat všech typů IP paketů nebo je možno zvolit z nabídky **IP protokol** určitý typ paketů: TCP, UDP, ICMP nebo „jiný“ (určený číslem protokolu). V závislosti na zvoleném protokolu je možné nastavit ještě další vlastnosti tohoto povolení: buď čísla povolených portů a druh paketu (pro TCP a UDP) nebo typ zpráv (pro ICMP).

Dále lze zvolit **Směr** paketů, a pokud definujete povolení pro určité konkrétní rozhraní (např. síťovou kartu), pak lze nastavit i další parametry:

- **Zdroj** – Jako zdroj lze nastavit libovolnou IP adresu s vyloučením konkrétních adres (tlačítkem ...), jednotlivou IP adresu, IP adresu definovanou adresou a maskou podsítě, IP adresu z rozsahu určeného počáteční a koncovou IP adresou.
- **Cíl** – možnosti určení cíle jsou analogické s definicí **Zdroje**.

Konfigurace odesílání a příjmu e-mailů (nastavení SMTP)

Messaging Server

V konfiguraci vyberte/přidejte SMTP službu a v jejím nastavení proved'te následující úpravy:

- na záložce Příjem zásilek se ujistěte, že máte zaškrtnutou volbu „Povolit relay faxů“, jinak by uživatelé SMTP/POP3 klientů nemohli odesílat faxy,
- při povolené **akceptaci vadných lokálních** adres budou zásilky se správnou doménou ale špatným jménem doručovány do složky Nezařazená pošta, do které mají přístup pouze uživatelé s právem „Rozdělování nezařazené pošty“, které jde nastavit ve vlastnostech jednotlivých uživatelů. V opačném případě je bude server vracet odesílatelům jako nedoručitelné.

- Pro zvýšení bezpečnosti doporučujeme nadefinovat IP filtr pro SMTP relay – zaškrtněte tuto volbu a po stisku tlačítka nadefinujte IP adresy a masky, pro které je SMTP relay povolen = kdo může odesílat poštu přes Váš SMTP server.

Příjem zásilek protokolem SMTP

SMTP protokol předpokládá, že daný SMTP server, na který doručuje zásilky, je vždy dostupný (tzn. je spuštěn a připojen k internetu). Jestliže nemáte trvalé připojení k internetu (např. používáte dial-up připojení), existují dvě možnosti řešení:

- Váš poskytovatel připojení může podporovat tzv. SMTP spooling – pokud není Váš SMTP server dostupný, může Váš poskytovatel dočasně uložit zásilky do fronty.
- Váš poskytovatel připojení nepodporuje SMTP spooling – zásilky jsou ukládány do POP3 schránky (zpravidla doménového koše), který Vám poskytovatel zřídil.

Nastavení protokolu SMTP

SMTP server můžete zapnout/vypnout zaškrtnutím stejnojmenné volby na záložce **Příjem zásilek**. Dále můžete specifikovat TCP/IP rozhraní, na kterém bude naslouchat. Standardně jsou zvolena **všechna rozhraní**, ale můžete vybrat i konkrétní **IP adresu** ze seznamu. To může být vhodné jak z provozních, tak bezpečnostních důvodů (můžete specifikovat pouze vnitřní IP adresu, která umožní přístup k SMTP serveru pouze lokálním uživatelům).

Messaging Server rovněž obsahuje i zabezpečený SSL SMTP server, který standardně pracuje na portu 2525.

Volba způsobu zpracování zásilek

Pro odesílání zásilek SMTP protokolem musí být na záložce **Odesílání zásilek** zaškrtnuta volba **Odesílání zásilek SMTP protokolem**.

Zásilky odesílat přes nadřizený SMTP server

Nejjednodušší způsob, jak odeslat zásilku do internetu, představuje přenesení problematiky vyhledání cíle pro zásilku a jejího doručení na jiný počítač v internetu, obvykle na SMTP server poskytovatele připojení. Stačí zaškrtnout volbu **Zásilky odesílat přes nadřizený SMTP server** na záložce **Odesílání zásilek** a pro odesílání budete moci využívat externí počítač, který ví, kam poštu doručit. Musíte znát jeho adresu, buď v IP nebo symbolickém (doménovém) tvaru a zapsat ji do pole **Nadřizený uzel**. Pokud je třeba zadat i číslo portu, uveďte ho za adresu serveru oddělené dvojtečkou.

Pozn. Možnost doručování přes nadřazený server doporučujeme využívat při dial-up napojení. Zásilky se maximální rychlostí přenesou k poskytovateli připojení, a teprve pak se vydají na „pomalou“ cestu internetem.

Přímé odesílání zásilek s využitím MX záznamů DNS

Pokud chcete zásilky odesílat přímo na cílové servery, můžete pro odesílání zásilek využít MX záznamy uložené v DNS, které mj. obsahují informace, kam se má pošta pro danou doménu doručovat. DNS požadavek posoudí a pokud přímo nenajde odpovídající MX záznam, postoupí jej „bližšímu“ DNS. To se opakuje, až je příslušný záznam nalezen a cílová adresa pro doručení sestavena.

Zkontrolujte, že na záložce **Odesílání zásilek** NENÍ zatržena volba **Zásilky odesílat přes nadřazený SMTP server**, a klikněte na tlačítko **Nastavení odesílání pro odborníky** a vyplňte položky **DNS1** a **DNS2** (pokud existuje) podle údajů od poskytovatele připojení. Pokud tyto parametry ne zadáte, Messaging Server použije DNS zadané v konfiguraci protokolu TCP/IP ve Windows.

Pozn. Tento způsob doručování doporučujeme používat při trvalém připojení k internetu.

Vyžádání zásilek u nadřazeného SMTP serveru

Pokud SMTP server Vašeho poskytovatele podporuje tzv. SMTP spooling, můžete přijímat zásilky pomocí SMTP serveru, i když nemáte trvalé připojení k internetu.

Při příjmu zásilek vytáčenou linkou prostřednictvím SMTP může být po dohodě s poskytovatelem zapotřebí vyslat příkaz **ETRN** k tomu, aby SMTP server poskytovatele začal vysílat zadržované zásilky pro „náš“ SMTP server.

V takovém případě zaškrtněte na záložce **Příjem zásilek** přepínač **při navázání dial-up připojení** a server specifikujte pomocí jeho adresy v poli **Nadřazený SMTP server**. Messaging Server pak vyšle ETRN příkaz při každém spuštění a při každém navázání dial-up připojení. Příkaz ETRN lze také vysílat periodicky každých X minut včetně potřebných parametrů.

SMTP RELAY

Funkce RELAY dovoluje SMTP serveru přijmout zásilku, jejíž adresát zde nemá schránku, a tuto zásilku je nutno odeslat dále jejímu adresátovi. Funkce je tedy nutná pro ty uživatele Messaging Server, kteří odesílají své zásilky z klientských SMTP/POP3 programů

(např. Outlook Express) do Messaging Server, který je např. po navázání dial-up napojení odešle do internetu.

Standardně je Messaging Server nastaven tak, aby službu RELAY poskytovala pouze pro své uživatele (je zatržena volba **Služba SMTP RELAY pouze pro uživatele**). SMTP server pak testuje adresy odesílatelů; pokud odesílatel nemá v Messaging Server účet (testuje se seznam uživatelských jmen včetně **aliasů**), SMTP server požadovanou službu neposkytne – nedovolí zasluku odeslat.

Pokud zatrhnete i volbu **Ověřovat pomocí předcházejícího POP3 přístupu**, dovolí SMTP server odesílat zasluky pouze uživatelům, kteří se maximálně před 120 minutami úspěšně přihlásili do své POP3 schránky.

POZOR! – Pokud není zaškrtnuta ani jedna volba, SMTP server, obzvláště je-li připojen k internetu pevnou linkou, je zneužitelný pro šíření nevyžádaných (SPAM) zasluk!

Pokud chcete přístup k funkci SMTP RELAY navíc chránit speciálním IP filtrem, zaškrtněte volbu **Pro přístup k SMTP RELAY platí IP filtr** a po stisku tlačítka **SMTP relay IP filtr** nastavte povolené či zakázané IP adresy.

Např. přístup k SMTP RELAY pouze v rámci Vaší lokální sítě povolíte zpravidla zadáním IP adresy 192.168.1.1 a masky 255.255.255.0 (přístup bude povolen ze všech počítačů s IP adresou 192.168.1.x).

Nastavení odesílání pro odborníky

Pomocí tohoto tlačítka umístěného na kartě **Odesílání zasluk** získáte možnost nastavit následující parametry:

Nadřizovaný SMTP server vyžaduje autentizaci

Někteří poskytovatelé připojení vyžadují před odesláním e-mailu přes jejich SMTP server autentifikaci. Pokud to Váš poskytovatel požaduje, zaškrtněte volbu **Nadřizovaný SMTP server vyžaduje autentizaci**. Dále zvolte způsob autentifikace – **SMTP** nebo **POP3** (způsob Vám sdělí poskytovatel) a vyplňte **Jméno** a **Heslo**. Server specifikujte pomocí jeho adresy v poli **Nadřizovaný uzel** na záložce **Odesílání zasluk**.

Nadřizovaný SMTP server vyžaduje zabezpečené spojení (SSL)

Někteří poskytovatelé připojení vyžadují, aby odesílatel komunikoval s jejich nadřizovým SMTP serverem přes spojení zabezpečené (šifrované) pomocí SSL. V tom

případě zaškrtněte stejnojmennou volbu a server specifikujte pomocí jeho adresy v poli **Nadřazený uzel** na záložce **Odesílání zásilek**.

Privátní síť a síť WAN

Směrování poštovních zásilek podle seznamu použijete v případě, že se zásilky do vyjmenovaných domén mají posílat přímo na určité počítače, narozdíl od ostatních zásilek, které budou doručovány do internetu podle MX záznamů v DNS nebo prostřednictvím SMTP serveru poskytovatele. Jako příklad použití uveďme doručování zásilek SMTP protokolem v síti WAN a do internetu.

Při zaškrtnutí čtverce **Směrování podle seznamu** v dialogu **Nastavení odesílání pro odborníky** se zpřístupní tlačítko **Přednastavená směrování**. Jeho stiskem se otevře pomocný dialog. Do polí **Poštovní doména** a **Cílový počítač** запиšte potřebné údaje a stiskněte tlačítko **Přidat**. Zadaná dvojice hodnot se zařadí do seznamu. Údaje v seznamu lze upravovat nebo mazat po nastavení ukazatele a stisku tlačítka **Vymazat/Editovat**.

Nastavení DNS

Vyplňte položky **DNS1** a **DNS2** (pokud existuje) podle údajů od poskytovatele připojení. Pokud tyto parametry ne zadáte, Messaging Server použije DNS zadané v konfiguraci protokolu TCP/IP ve Windows (viz výše **Přímé odesílání zásilek s využitím MX záznamů DNS**).

Pracovní intervaly

Nastavení pracovních intervalů pro SMTP server:

- **Doba mezi dvěma pokusy o odeslání zásilky** – pokud nemůže být zásilka odeslána (např. cílový SMTP server je mimo provoz), bude pokus o odeslání opakován po uplynutí zadané doby (v minutách).
- **Nedoručitelnou zásilku odložit po** – může se také stát, že se zásilku nezdaří doručit ani při dalších pokusech. Tento parametr udává interval v hodinách, po kterém je nedoručitelná zásilka definitivně odložena.

Max. počet současných SMTP vysílání

Hodnota položky **Max. počet současných SMTP vysílání** v okně **Nastavení odesílání pro odborníky** určuje, kolik může být zároveň navázáno SMTP spojení pro vysílání zásilek. To umožňuje regulovat zatížení komunikační linky.

Parametr příkazu HELO/EHLO

SMTP relace mezi SMTP servery začíná příkazem HELO (resp. EHLO u ESMTP), za kterým má následovat jméno volajícího serveru. SMTP server v Messaging Server implicitně čte toto jméno z konfigurace Windows. Pokud jsou s konfigurací tohoto jména nějaké potíže nebo je třeba, aby se tento server představoval pod jiným jménem (např. při volání z vnitřní sítě přes NAT nebo mapované spojení na jiném počítači), je možné tento parametr explicitně zadat v této vstupní řádce.

Antispamové nastavení pro SMTP příjem

Stiskem tlačítka **Anti-Spam nastavení** na záložce **Příjem zásilek** se otevře dialog, ve kterém můžete potlačit příjem nežádoucích, zejména reklamních zásilek (tzv. spamů).

Upozornění: Toto nastavení se týká pouze příjmu zásilek protokolem SMTP a nijak tedy neovlivňuje zásilky stahované z POP3 schránek.

Použit zvolené vyhledávací DNSBL služby k odmítnutí zásilek od spamovacích serverů

V okně je zobrazen seznam serverů, které se zabývají odhalováním a evidencí serverů rozesílajících spamy. Seznam je sestaven za mezinárodní spolupráce poskytovatelů připojení. Pokud zaškrtnete čtverec před názvem položky, příjem každé zásilky bude nejprve danou službou posouzen a případně odmítnut. Některé servery poskytují své služby zdarma a některé ne (PLATÍ SE). Seznam si můžete sami upravit pomocí trojice tlačítek **Přidat službu**, **Editovat službu** a **Smazat službu**.

U každé služby můžete nastavit:

- **Jméno služby** – popisné jméno
- **Vyhledávací doména** – doména, kde je služba provozována
- **IP adresa vrácená v případě nalezení v seznamu** – návratovou adresu definuje poskytovatel antispam služby. Je vrácena SMTP serveru v případě nalezení odesílacího serveru v databázi.
- **Text zamítnutí** – tento text je zaznamenán do log souboru v případě, že je příchozí zásilka označena danou službou jako spam.

Odmítnout zásilky od těchto serverů nebo odesílatelů

Pomocí tlačítek **Přidat**, **Editovat** a **Smazat** si můžete vytvořit seznam adres, ze kterých nebudete přijímat žádné zásilky. Lze zadat konkrétní e-mailovou adresu, adresu serveru nebo

použít zástupné znaky * a ?. Seznam můžete také importovat i exportovat ve formě textového souboru, kde na každé řádce je jeden server nebo odesílatel.

Nikdy neodmítat zásilky od těchto serverů nebo odesílatelů

Zde můžete analogicky předchozímu bodu vytvořit seznam odesílatelů a serverů, jejichž zásilky nebudete nikdy odmítat (nepovažujete je za spam). Tohoto nastavení lze s výhodou využít, pokud nastavíte odmítání zásilek např. od celé domény *.ru a přitom ale chcete přijímat zásilky od odesílatele oleg@posta.ru. To zajistíte tak, že ho přidáte do tohoto seznamu.

Konfigurace příjmu e-mailů (nastavení POP3)

Administrátor

Pokud budete chtít využívat pro přístup do pošty programy pracující na bázi protokolu POP3 (např. MS Outlook Express, Netscape Messenger, ...), je třeba ve vlastnostech uživatele zaškrtnout volbu „Vybírání POP3 protokolem povoleno“. To lze samozřejmě provést i hromadně, pokud označíte více uživatelů.

Messaging Server

V konfiguraci vyberte/přidejte POP3 službu. **POP3 server** následně zapnete zaškrtnutím stejnojmenné volby. Dále můžete specifikovat TCP/IP rozhraní, na kterém bude POP3 server naslouchat. Standardně jsou zvolena **všechna rozhraní**, ale můžete vybrat i konkrétní **IP adresu** ze seznamu. Standardní port pro POP3 server je 110, můžete ho ale v případě potřeby změnit (je ale pak nutné provést obdobnou změnu i v konfiguraci klientských programů).

Messaging Server také obsahuje zabezpečený SSL POP3 server. Jeho konfigurace je shodná jako u standardního POP3 serveru. Standardně je spouštěn na portu 995

Pokud chcete, aby Messaging Server v pravidelných intervalech stahoval poštu z POP3 schránek na Internetu, nastavte tyto schránky spolu s jejich parametry na záložce „Výběr POP3 schránek na internetu“.

Výběr POP3 schránek na internetu

Do **Seznamu POP3 schránek, které mají být pravidelně vybírány** můžete tlačítkem **Přidat** snadno doplnit další schránku. Již zadané schránky můžete tlačítky vpravo **Editovat** nebo **Vymazat**.

Základní parametry pro výběr POP3 schránky

Při zadávání nové (editaci stávající) vybrané POP3 schránky je třeba zadat následující údaje (sdělí Vám je zpravidla poskytovatel připojení):

- **POP3 server** – adresa serveru na internetu s danou POP3 schránkou
Někteří poskytovatelé připojení vyžadují, aby program komunikoval s jejich POP3 serverem přes spojení zabezpečené (šifrované) pomocí SSL. V tom případě zaškrtněte volbu **Server vyžaduje zabezpečené připojení (SSL)**.
- **Přihlašovací jméno** – jméno schránky (uživatelské jméno)
- **Heslo** – přihlašovací heslo

Použit APOP

Pokud nastavíte volbu **Použit APOP** na **Ano**, bude při přihlašování do POP3 schránky místo nezakódovaného hesla zaslán pouze jeho otisk v řetězci náhodných znaků, což zvyšuje bezpečnost. Záleží na poskytovateli schránky, zda tuto možnost podporuje. Standardně je tato volba nastavena na **Ne**.

Třídění přijatých zásilek

Pomocí volby **Přijaté zásilky doručit** můžete specifikovat, komu budou doručovány zásilky získané z dané POP3 schránky.

Pokud zvolíte možnost **podle adres v dopisu** budou zásilky automaticky doručovány uživatelům podle adresy (tj. bude se kontrolovat adresa adresáta proti uživatelskému jménu a doméně nastavené v poštovním úřadě a následně proti nastaveným aliasům). Tak lze například nechat server automaticky doručovat poštu z tzv. doménového koše. Pokud se jedná o standardní zásilku adresovanou jedné osobě, adresa se v hlavičce dopisu najde a podle ní se zásilka doručí.

Složitější situace nastává u zásilek, které jsou adresovány více osobám, jsou adresovány pomocí položky skryté kopie, jsou to zásilky z konferencí nebo jsou v průběhu cesty doručovány nestandardními poštovními servery. Obvykle se u takových zásilek najde správná adresa adresáta v položce „for“ a tato informace má přednost před ostatními klíči. Pokud zjistíte, že tento postup rozboru zásilek nevyhovuje, použijte **podle adres v dopisu – alternativní metoda**, kde již položka „for“ přednost nemá a použijí se k rozboru i ostatní klíče uvedené v hlavičce.

Druhou možností je doručování konkrétnímu uživateli bez ohledu na adresu v dopise. V tom případě zvolte ze seznamu **Přijaté zásilky doručit** konkrétního uživatele.

Interval výběru schránky

Časový interval kontaktování POP3 schránky s cílem vybrat její obsah nastavíte přepínačem **Kdy vybírat schránku**:

- **každých X minut** – schránka bude vybírána v pravidelných časových intervalech, vždy po uplynutí X minut
- **v určených časech** – schránka bude vybírána v určené hodiny a minuty; seznam časových údajů zapíšete do pole vedle sebe oddělíte čárkou, například 7:00, 9:00, 12:00, 13:00...atd.

Další omezení výběru POP3 schránek s ohledem na navazování připojení lze nastavit na záložce Připojení.

Ponechání zásilek na serveru

Standardně se zásilky vybrané z POP3 schránky ze serveru na internetu odstraňují. Pokud je chcete na serveru ještě nějakou dobu ponechat, můžete do pole **Ponechat vybrané zásilky na serveru po dobu X dní** zapsat počet dnů, kolik se má ve schránce na serveru uchovat originál zásilky, jejíž kopie již byla vložena do lokální schránky adresáta. Pokud zde zapíšete nulu, budou se zásilky z internetu adresátům do schránek přímo přesouvat aniž by vznikaly kopie.

Nastavení Messaging Serveru pro SSL SMTP/POP3

Zabezpečení SMTP a POP3 serveru pomocí SSL zabraňuje mj. „odposlechu“ Vašeho hesla i Vašich e-mailů na cestě mezi SMTP/POP3 serverem a Vaším počítačem. Pro využití těchto funkcí je třeba, aby je podporoval jak server tak i klient.

Nejprve je třeba v Messaging Serveru vygenerovat klíče pro SSL komunikaci. To lze udělat např. v nastavení SMTP služby, kdy po stisku tlačítka „Nastavení SSL“, následně tlačítka „Vytvořit soukromý a veřejný klíč“ a zadání několika údajů budou tyto klíče automaticky vygenerovány.

Potom již stačí zaškrtnout volbu „SSL SMTP server“ v nastavení služby SMTP resp. volbu „SSL POP3 server“ v nastavení služby POP3.

Antivirová kontrola zásilek

Messaging Server

Vestavěnou antivirovou kontrolu (systémem BitDefender™) zapnete zaškrtnutím volby **Provádět kontrolu zásilek antivirovým systémem Mail602** na záložce **Antivirová kontrola** v Konfiguraci pro odborníky (tato volba je aktivní pouze pokud máte zakoupenou příslušnou licenci). V případě, že je v příchozí zásilce detekován vir, záleží na nastavení dalších voleb na kartě.

Standardně antivirový systém Messaging Server nerozlišuje mezi podezřelými a infikovanými zprávami. Pokud chcete, aby antivirová kontrola ignorovala zprávy, u kterých bylo podezření na přítomnost viru detekováno pomocí heuristické analýzy, zrušte zaškrtnutí volby **Mail602 MESSAGING SERVER antivirus: Nakládat s podezřelými zprávami stejně jako s infikovanými**.

V případě nakažené příchozí zprávy

Poznámka: Pokud není pro danou situaci zaškrtnuta žádná z voleb (a antivirová kontrola je zapnuta), není zavirovaná zpráva doručena nikomu a je rovnou odstraněna (bez odeslání upozorňovacího e-mailu).

Server může **Zaslat adresátům vyrozumění o závadné zprávě** (pouze upozorňující e-mail, že jim odesílatel poslal zavirovanou zprávu). Toto upozornění může být odesíláno pouze administrátorům, při zaškrtnutí příslušné volby.

Pokud je zaškrtnuta i volba **Včetně závadné zprávy**, bude upozorňovací zpráva obsahovat i původní zprávu (tj. včetně zavirovaných souborů!). Proto lze platnost této volby opět omezit pouze na administrátory poštovního úřadu.

Kromě upozorňovacího e-mailu může být každá zavirovaná zpráva doručena také **do speciální schránky**, kterou vyberete ze seznamu vpravo. Je vhodné zvolit např. schránku, u které se předpokládá, že je pro tento účel vyčleněna a spravuje ji tedy uživatel dobře seznámený s antivirovou problematikou.

Certifikace

Po zaškrtnutí volby **Certifikovat příchozí e-mailové zprávy** bude na konec všech přijímaných zpráv automaticky vkládán text, který zadáte do editačního pole **Certifikační text doplněný do příchozích zpráv**.

Aktualizace

Messaging Server umožňuje provádět v pravidelných intervalech automatickou aktualizaci vestavěného antivirového systému BitDefender™. To lze nastavit pomocí volby **Provádět automatickou aktualizaci antiviru každých X hodin**.

Pokud v okamžiku vypršení intervalu pro aktualizaci není navázáno dial-up připojení k internetu, provede Messaging Server aktualizaci okamžitě po jeho dalším navázání.

Pokud pro spojení do internetu používáte nadřazený proxy server, uveďte jeho adresu do řádku **Použít HTTP proxy**. Pokud je třeba zadat i číslo portu, uveďte ho za adresu serveru oddělené dvojtečkou.

V případě potřeby je možno provést aktualizaci okamžitě stiskem tlačítka **Provést aktualizaci**.

AVG

Pokud máte na stejném počítači s Messaging Server nainstalován antivirový systém AVG (verze 6 nebo 7), můžete ho při dodržení licenčních podmínek využít ke kontrole přijímaných zásilek.

Antivirovou kontrolu zapnete zaškrtnutím volby **Provádět kontrolu doručovaných zásilek antivirovým systémem AVG** na záložce AVG. V případě, že je v příchozí nebo odchozí zásilce detekován vir, záleží na nastavení dalších voleb na kartě **Nastavení**.

Pozn. Messaging Server nekontroluje ani neprovádí automatické aktualizace systému AVG.

Filtrace příloh

Filtr nebezpečných příloh snižuje riziko příjmu e-mailů obsahujících například zcela nový počítačový virus a lze ho také využít pro filtraci souborů zjevně nesouvisejících s pracovní náplní uživatelů.

Filtrace příloh zásilek podle koncovek

Příchozí i odchozí zásilky je možné filtrovat podle přípon připojených souborů. Tento filtr jednak zvyšuje antivirovou bezpečnost sítě odstraněním spustitelných souborů a zároveň snižuje možnosti zneužití firemního emailového systému k soukromým účelům např. odstraňováním připojených souborů AVI, MP3 apod.

Zaškrtnutím volby **Filtrace přílohy zásilek podle koncovek** na záložce **Filtrace příloh** v Konfiguraci pro odborníky tento filtr zapnete. Dále lze v zadávacím okně specifikovat

koncovky nežádoucích příloh oddělené čárkou, přičemž lze použít i zástupné znaky * a ? (např. DO? znamená DOC, DOT, DOP atd.). Ve výchozím stavu obsahuje okno většinu nebezpečných (spustitelných) příloh, které by se neměly vyskytovat jako běžná příloha e-mailů. Do tohoto výchozího stavu se lze kdykoliv vrátit zpět stiskem tlačítka **Výchozí**, které zruší všechny provedené změny v seznamu přípon a uvede jej do výchozího stavu.

Seznam přípon můžete libovolně editovat, a to buď přímo nebo prostřednictvím tlačítka „...“, po jehož stisku dojde k načtení seznamu přípon spolu s jejich popisem z registrační databáze. Následně můžete v zobrazeném dialogu přílohy zaškrtnout a pomocí příslušných tlačítek označit/odznačit všechny přípony nebo již provedený výběr invertovat.

Pozn. Filtr testuje pouze koncovky souborů, nikoliv jejich obsah.

Omezení účinnosti filtru

Zaškrtnutím příslušných voleb lze omezit účinnost filtru tak, aby se nefiltrovaly:

- **zásilky pro administrátory** – filtr nebude kontrolovat zásilky doručované uživatelům s administrátorskými právy
- **zásilky od administrátorů** – filtr nebude kontrolovat zásilky odesílané uživateli s administrátorskými právy
- **lokální zásilky** – filtr nebude kontrolovat zásilky mezi lokálními uživateli

Nastavení akce při nalezení nežádoucí přílohy

V případě, že filtr nalezne v zásilce nežádoucí přílohu, může s ní nebo celou zásilkou provést různé činnosti. Ty se specifikují zvláště pro přijímané a odesílané zásilky.

Zpracování příchozích zásilek

Na záložce **V případě příchozí zásilky** lze určit, co se má stát s příchozí zásilkou, ve které byla nalezena nežádoucí příloha. Zásilku je možno adresátovi:

- **Doručit** – zásilka bude doručena původnímu adresátovi včetně všech příloh
- **Doručit bez nežádoucích příloh** – zásilka bude doručena původnímu adresátovi, ale bez nežádoucích příloh, které budou v zásilce nahrazeny informačním sdělením
- **Nedoručit** – zásilka nebude původnímu adresátovi vůbec doručena, a pokud nebude nastaveno její doručení do zvláštní schránky, bude celá vymazána

Zaškrtnutím volby **Doručit zásilku do speciální schránky** lze zajistit, aby i v případě, že zásilka nebude doručena původnímu adresátovi, bylo možno prozkoumat její obsah pověřeným uživatelem.

Zpracování odchozích zásilek

Na záložce **V případě odchozí zásilky** lze specifikovat, zda se má zásilka obsahující nepovolené přílohy adresátovi:

- **Doručit** – zásilka bude adresátovi odeslána včetně všech příloh
- **Nedoručit** – zásilka nebude vůbec odeslána a bude vrácena zpět odesilateli s informací, že se pokouší odeslat zásilku s nepovolenou přílohou

Antispam

Na záložce **Antispam** v Konfiguraci pro odborníky se konfiguruje chování bayesovského filtru, který analyzuje obsah zásilky a klasifikuje ho mírou pravděpodobnosti, že daná zásilka je spam.

Princip fungování bayesovského filtru

Bayesovský filtr analyzuje obsah přijímané zásilky a klasifikuje ho mírou pravděpodobnosti, že daná zásilka je nevyžádaná zásilka (spam). Tuto činnost provádí na základě porovnání slov v obsahu zásilky s obsahem své databáze, kam zařazuje slova ze zásilek, které uživatel již dříve označil za spam nebo naopak za vyžádané zásilky. Z toho plyne, že filtr je třeba nejdříve „naučit“, tedy naplnit jeho databázi zásilkami, o nichž sám uživatel rozhodne zda jsou či nejsou spamem. Učení může probíhat manuálně i automaticky z odpovědí na zásilky.

Aby filtr dosáhl dobré filtrovací schopnosti, potřebuje se naučit nejprve desítky či spíše stovky jak spamových tak ne-spamových zásilek. Protože neexistuje jasná definice spamu a jednomu uživateli se stejná zásilka může jevit jako spam a druhému jako zajímavá obchodní nabídka, nedodáváme bayesovský filtr již naplněný a záleží jen na uživateli, které zásilky bude označovat za nevyžádané.

Původní algoritmus bayesovského filtru vytvořil Paul Graham, bližší popis lze získat např. na <http://spambayes.sourceforge.net>.

Pozn. Narozdíl od **Anti-Spam nastavení**, které se nastavuje v konfiguraci služby SMTP a které ovlivňuje pouze zásilky přijímané protokolem SMTP, bayesovský filtr pracuje se všemi zásilkami – tedy i zásilkami vybíranými z POP3 schránky.

Konfigurace bayesovského filtru

Administrátor může globálně **Povolit používání bayesovského filtru pro kontrolu došlých zásilek** zaškrtnutím stejnojmenné volby. Dále může nastavit, jaké míry

pravděpodobnosti, že se jedná o nevyžádanou zásilku (spam), musí zásilka dosáhnout, aby byla bayesovským filtrem označena za spam. To lze specifikovat v položce **Klasifikovat zásilku jako SPAM, pokud přesáhne skóre X %**.

Antispamová schránka

V konfigurační kartě Antispam je také možné nastavit tzv. **Antispamovou schránku**. Může se jednat o zcela zvláštní schránku nebo to může být schránka administrátora popř. uživatele pověřeného touto činností. Tato schránka má dvě základní použití:

- Při odpovídajícím nastavení do ní budou doručovány zásilky označené jako spam a daný uživatel bude pouze pravidelně kontrolovat zda mezi nimi nejsou i zásilky, které spamem nejsou (viz nastavení na kartě **Akce**).
- V závislosti na nastaveném způsobu **Učení bayesovského filtru** mohou do Antispamové schránky docházet buď žádosti uživatelů o naučení připojené zásilky jako spamu nebo ne-spamu (legitimní zásilky) nebo sem mohou přicházet zprávy o tom, že se bayesovský filtr připojenou zásilku naučil a obsluha může v případě potřeby způsobit opačnou akci (zásilku odnaučit).

K práci s Antispamovou schránkou lze s výhodou využít program Mail602 Klient nebo webové rozhraní pro práci s poštou.

Kontrolovat i zásilky retranslované dalším úřadům

Zaškrtnutím této volby určíte, že má Messaging Server kontrolovat pomocí bayesovského filtru i zásilky, které jsou určeny pro podřízené poštovní úřady a na které jsou tyto zásilky po přijetí z internetu retranslovány protokolem Mail602.

Nastavení akce, pokud je zásilka klasifikována filtrem jako spam

Na záložce **Akce** lze určit, co se stane, pokud je zásilka klasifikována bayesovským filtrem jako spam. V závislosti na tomto nastavení může server zásilku:

- **Smazat** – zásilka bude nenávratně vymazána. Doporučujeme používat jen při řádně naučeném bayesovském filtru a až po ověření jeho spolehlivé funkčnosti.
- **Zaslat adresátovi** – zásilka je normálně doručena původnímu adresátovi, přičemž je modifikována podle dalších nastavení na záložce.
- **Zaslat do Antispamové schránky** – zásilka je doručena do speciální Antispamové schránky, přičemž je modifikována podle dalších nastavení na záložce.

Pro přehled a třídění došlých zásilek v klientských programech je vhodné v zásilkách označených jako spam doplňovat pole předmět o nějaký řetězec říkající, že jde o nevyžádanou zasilku. Toho lze docílit zaškrtnutím volby **Označovat spamy vložení tohoto řetězce do předmětu zasilky** a jeho zadáním. Zadaný řetězec může být alternativně vkládán **na začátek předmětu** nebo **na konec předmětu**.

Server může také volitelně **Vkládat do hlavičky kontrolovaných zásilek pole X-602-SpamCheck s informací o výsledku kontroly**, ze kterého lze případně zjistit, proč byla nebo naopak nebyla zasilka označena bayesovským filtrem jako spam.

Pozn. Pro zobrazení tohoto pole v klientském poštovním programu je třeba si nechat zobrazit úplnou hlavičku zasilky – např. v programu Mail602 Klient v otevřené zasilce přes menu Zobrazit – Záhloví dopisu, nebo třeba v Outlook Express v otevřené zasilce přes menu Soubor – Vlastnosti – záložka Podrobnosti; ve webovém rozhraní si v Nastavení přepněte volbu Hlavička prohlížené zasilky na Plná.

Učení bayesovského filtru

Označování zásilek uživateli

Bayesovský filtr mohou učit uživatelé prostřednictvím označování zásilek jako **Spam** nebo **Nesbam** v prostředí programu Mail602 Klient, webového rozhraní nebo obdobnou akcí ve svém POP3 klientském programu (např. Outlook Express) prostřednictvím přeposílání nevyžádaných zásilek (spamů) na adresu **spam@spam** a vyžádaných (normálních) zásilek na adresu **notspam@spam**.

Automatické učení podle „bílé listiny“

Další možností je automatické učení bayesovského filtru ze zásilek, které přicházejí od odesílatelů z internetu a kteří jsou již uvedeni na uživatelské „Bílé listině“ adresáta. Každý uživatel si může ve webovém rozhraní sám spravovat svou bílou listinu odesílatelů, jejichž zasilky nebudou nikdy považovány za spam. Pokud chcete aby se filtr sám učil ze zásilek těchto odesílatelů, zaškrtněte na záložce **Učení bayesovského filtru** volbu **Automaticky naučit zasilky od odesílatelů uvedených na „bílé listině“ adresáta**.

Možnosti zpracování žádosti o naučení zasilky

Další nastavení na záložce **Učení bayesovského filtru** definuje způsob zpracování žádosti uživatele o naučení právě označené (přeposlané) zasilky:

- **se zasilka naučí** – filtr se obsah zasilky okamžitě naučí

- **se zázilka naučí a do antispamové schránky se vloží oznámení** - filtr se obsah zázilky okamžitě naučí, ale pošle do antispamové schránky oznámení, které umožní pověřenému uživateli provést dodatečnou kontrolu zázilky a v případě potřeby ji filtr opět „odnaučit“
- **se do antispamové schránky vloží žádost o naučení** – filtr se obsah zázilky nenaučí, pošle žádost do antispamové schránky a čeká, zda tuto žádost schválí pověřený uživatel

Zálohování databáze bayesovského filtru

Bayesovský filtr si ukládá svá data do souborů mails.db a words.db v adresáři s programem Messaging Server. Zejména při automatickém nebo přímém učení filtru je vhodné pravidelně provádět zálohy těchto souborů pro případ, že dojde k nesprávnému naučení většího množství zázilek a je třeba se vrátit ke staršímu stavu databáze slov.

Na záložce **Záloha databáze filtru** je zobrazován aktuální stav databáze – tj. její velikost v KB a počet naučených spamů a ne-spamů. Tlačítkem **Uložení databáze bayes. filtru** lze provést zálohu databáze, její zpětné obnovení pak provedete tlačítkem **Načtení databáze bayes. filtru**.

Přístup na internet pomocí překladu adres (NAT)

Překlad IP adres v paketech neboli NAT (Network Address Translation) umožňuje připojení stanic s vnitřní IP adresou v lokální síti k internetu na paketové úrovni. NAT stejně jako firewall pracuje, pouze pokud je Messaging Server provozován na Windows 2000/2003 a XP.

Princip fungování NAT

V paketech jdoucích z chráněné vnitřní sítě do internetu je původní (privátní) zdrojová IP adresa nahrazována veřejnou IP adresou vnějšího rozhraní počítače s Messaging Server. Do internetu tedy odcházejí pouze pakety s IP adresou tohoto počítače jako odesilatele paketu – z paketu tedy nelze zjistit IP adresu původního odesilatele, čímž zůstávají počítače za NAT skryty. O paketech odeslaných do internetu je zároveň vytvořen záznam v tzv. NAT tabulce.

Každý paket přijatý z internetu je pak porovnán se záznamy v NAT tabulce. Je-li nalezen odpovídající záznam, provede se změna cílové IP adresy v tomto paketu na IP adresu příslušného počítače ve vnitřní síti a paket je na tento počítač poslán. Tím je zajištěno, že odpověď na vyslaný paket je správně doručena vysílajícímu počítači.

NAT je přístupný, pouze pokud je Messaging Server provozován na Windows 2000/2003 a XP. Konfigurace NAT předpokládá existenci alespoň dvou síťových rozhraní.

Výhody používání NAT

Z uvedeného popisu vyplývá, že není možné se z internetu spojit na počítač ve vnitřní síti. NAT tedy z principu chrání počítače ve vnitřní síti proti přístupu zvenčí.

Při používání NAT odpadá nutnost nastavovat na stanicích v síti ve všech aplikacích, které mají přistupovat na internet, adresu proxy nebo SOCKS serveru. Navíc některé aplikace ani přístup na internet skrz proxy nepodporují, a proto je bez využití NAT nelze používat.

Nevýhody používání NAT

Nevýhodou používání NAT pro přístup na internet je skutečnost, že nelze příliš ovlivňovat kdo, kdy a kam má nebo nemá mít přístup. Omezení lze v tomto případě definovat jedinečně pomocí IP filtru na úrovni vstupních a cílových IP adres.

Vyšší kontroly nad využíváním připojení k internetu proto dosáhnete, pokud budete pro přístup na internet využívat služeb HTTP proxy, kde lze využít autentifikace uživatelů pomocí hesel.

NAT – konfigurace

Aby NAT fungoval, je třeba mít na stanicích v síti nastavenou v konfiguraci TCP/IP výchozí bránu na IP adresu počítače s Messaging Server.

NAT se zapíná přidáním služby **NAT** a následným nastavením **Sdíleného rozhraní**, které slouží k připojení na internet. Dále je třeba vybrat **Překládaná rozhraní/podsítě** – tj. vnitřní rozhraní, na kterých bude překlad adres pracovat. Pokud má počítač více rozhraní do vnitřní sítě nebo mají tato rozhraní více IP adres, lze v jejich seznamu křížkem označit, pro která konkrétní rozhraní a jejich podsítě se má překlad adres provádět.

Pozn. Nejprve je vždy třeba zvolit **Sdílené rozhraní** a teprve potom **Překládané**.

Poznámky

- NAT podporuje příkaz *ping*, nepodporuje ale příkaz *tracert*,
- zatím nepodporuje také např. NetMeeting, IPsec, UPnP,
- provoz NATu nenavazuje dial-up spojení,
- mezi dvěma lokálními rozhraními se IP adresy nepřekládají.

Řízení přístupu k NAT – IP filtr

Pro řízení přístupu k funkci NAT lze použít **IP filtr**, který se nastavuje stejnojmenné podzáložce karty **NAT**. Podrobný popis nastavení a funkce IP filtru naleznete v kapitole **Proxy – IP filtr**, neboť princip konfigurace je zcela stejný.

Zde ovšem platí, že pokud v IP filtru není žádné pravidlo, je vše povoleno; pokud ale je v IP filtru alespoň jedno pravidlo, je vše ostatní zakázané.

Konfigurace sdíleného přístupu k Internetu (proxy)

Přístup k Internetu z lokální sítě kromě NATu zajišťuje také služba Proxy. Veškeré požadavky od klientských programů (stanic) procházejí komunikačním serverem, a proto se nejnázne využívají aplikace s vestavěnou podporou Proxy nebo SOCKS (v ostatních případech je třeba nakonfigurovat tzv. Mapované spojení nebo použít NAT – viz další text).

Nastavení Proxy

V nastavení služby Proxy v Messaging Serveru lze hned na první záložce konfigurovat běžně používané proxy brány, mezi které patří zejména HTTP/HTTPS/HTTP-FTP využívaná browsery pro přístup k WWW serverům na Internetu. Ve Vámi používaném browseru stačí uvést jako adresu proxy serveru IP adresu komunikačního serveru a port číslo 80.

SOCKS proxy verze 4 a 5 není závislá na používaném protokolu, a proto ji lze využít např. pro program ICQ nebo pro aplikace přenášející libovolná i kódovaná data.

Narozdí od HTTP-FTP proxy na portu 80 sloužící pro browsery je FTP proxy na portu 21 určena pro využití přímo z FTP klientských programů (např. WS_FTP, Cute FTP apod.).

Tab. 1 Nastavení běžných FTP klientů pro používání FTP proxy

| | |
|---|---|
| <p>CuteFTP</p> <p>Host : IP adresa MSG</p> <p>Type : user@site</p> <p>Enable firewall access</p> | <p>WS_FTP Pro</p> <p>Use firewall</p> <p>Host name : IP adresa MSG</p> <p>User with no logon</p> |
| <p>FTP Explorer</p> <p>Use Firewall</p> <p>Host : IP adresa MSG</p> <p>Firewall type : user@hostname</p> | <p>FAR file manager</p> <p>Firewall:port : IP adresa MSG</p> |

Dále je podporována Telnet proxy pro využívání programu Telnet skrz komunikační server. V programu Telnet lze zadat spojení na IP adresu komunikačního serveru, který Vás následně vyzve k zadání cílové adresy a portu.

RealAudio proxy umožňuje na stanicích v lokální síti, které jsou připojeny k Internetu pouze pomocí proxy, přehrávat multimediální klipy z Internetu pomocí programu RealPlayer firmy RealNetworks.

DNS proxy předává DNS požadavky ze sítě DNS serveru v Internetu a zpět vysílá odpovědi, čímž je pro všechny aplikace v síti plně zajištěna funkce DNS. Stanice v síti LAN ale často generují "zbytečné" DNS požadavky, kvůli kterým se pak navazují dial-up spojení. Pokud je tomu třeba předejít, zaškrtněte volbu "Nenavazovat dial-up spojení kvůli DNS". DNS proxy pak pracuje pouze v případě, že je dial-up spojení již navázáno z jiného důvodu.

Sledování činnosti Proxy serveru

Na záložce Zprávy lze kromě standardního zapnout i zaznamenávání operací s cache a prováděných proxy serverem ve formátu W3C, čehož lze využít pro následnou analýzu některým z komerčně dostupných programů.

Nastavení Proxy pro odborníky

Kromě změny portů, na kterých jsou v provozu příslušné druhy proxy, lze nastavit i parametry vyrovnávací paměti (cache).

Perioda úklidu cache udává časový interval v minutách, po kterém bude obsah vyrovnávací paměti testován a uvolněn vymazáním souborů s prošlou expirační lhůtou.

Expirační doba souborů v cache je doba v hodinách, po které budou soubory uložené ve vyrovnávací paměti vymazány.

Některé WWW a FTP servery nesdělují klientským programům velikost souborů a další informace. Pak se může stát, že při přerušení spojení v cache zůstane nekompletní soubor. Pokud povolíte volbu „Vyžadovat informace o souborech“, nebudou se soubory bez připojených informací do cache ukládat.

Při zapnuté volbě „Skripty (CGI, ASP) vždy provádět“ se proxy pokusí podle URL adresy zjistit, zda je daná HTML stránka produktem CGI skriptu a neuloží ji do cache, aby se při příštím pokusu o stažení znovu aktivoval CGI skript a do browseru se neposlala tedy stránka uložená v cache paměti.

Vysílající WWW server může vložit do hlaviček přenášených informací příkazy specifikující, jakým způsobem má být s příslušnou stránkou nakládáno. Obvykle se browseru

a proxy přikazuje, aby stránka nebyla vkládána do cache nebo se vymezuje její časová platnost. Pokud přepínač „Povolit řízení cache HTTP příkazy“ nezaškrtnete, proxy (a cache) tyto příkazy ignoruje.

Nadřazený proxy/cache server: HTTP proxy server obvykle přijímá data z cílových serverů. V některých případech je vhodné nastavit vícestupňovou proxy, kdy pak jeden proxy server žádá data po nadřazeném serveru. Typicky se jedná o využití velké proxy cache provozovatele internetového napojení.

Mapované spojení

Funkce „mapovaná spojení“ představuje alternativu pro napojení stanice privátní sítě k Internetu. Je vhodná pro použití z aplikací, které nepodporují SOCKS ani proxy a spojují se na konkrétních portech pouze s jedním počítačem v Internetu (např. připojení k serveru s diskusními příspěvky - news). Mapované spojení lze provádět protokolem TCP nebo UDP v Messaging Serveru v nastavení služby Proxy na příslušné záložce.

Pokud tedy klientský program na stanici v privátní síti potřebuje navázat TCP/IP spojení s konkrétním počítačem v Internetu, zadá se místo adresy tohoto počítače v klientském programu adresa Messaging Serveru, ve kterém se na kartě Mapovaná spojení určí, že pokud se na daný port připojí tato stanice, mají se všechny pakety posílat na určitý počítač v Internetu. Tím se vytvoří virtuální spojení mezi počítači prostřednictvím počítače s Messaging Serverem. Jedná se tedy o jakýsi přesměrovávač, jehož prostřednictvím se mohou po TCP/IP spojit dva počítače.

Výhodou je, že klientský program nemusí podporovat žádný typ proxy. Vlastností (nevýhodou) pak je, že se stanice takto může připojit pouze na jediný počítač v Internetu, resp. na ty počítače, které jsou konkrétně vypsány v Messaging Serveru.

Na kartě Mapovaná spojení je tedy nutné:

- Voličem Protokol vybrat, jakým protokolem se má spojení realizovat (TCP nebo UDP).
- Ve sloupci Spojení z – který počítač se bude připojovat (pole IP adresa a IP maska).
- Ve dvojici polí Na tento počítač – přes který port počítače bude navazován kontakt s Messaging Serverem (pole IP adresa a Port).
- Ve dvojici polí Mapovat na – na který počítač se má toto spojení směřovat (pole Cílová adresa a Port).

Zdrojový počítač s maskou a IP adresa počítače s Messaging Serverem musí být uvedeny číselnou IP adresou; číslo jeho portu a adresa a port cílového počítače mohou být uvedeny i symbolicky.

Pozn. Formát tabulky tedy umožňuje i takové nastavení, kdy se přes jeden port počítače s Internet Serverem může současně spojovat více počítačů na několik různých cílových počítačů, protože definujeme, který zdrojový počítač (sít') se má spojovat na který cílový počítač.

Pozn. Pokud počítači s Messaging Serverem přiřadíte více IP adres, můžete např. zpřístupnit více než jeden NEWS server na Internetu; vždy jeden server na jedno napojení, přičemž všechny užívají stejný NEWS port (ve střední části tabulky zadejte nejen číslo portu, ale i IP adresu). Pokud chcete, aby mapované spojení pracovalo současně na všech IP adresách tohoto počítače, zadejte tuto adresu jako 0.0.0.0. Jiným řešením je použití pro stejnou IP adresu různá čísla portů.

Příklad použití pro News

Následující příklad definuje, že všechny počítače z jedné podsítě budou přes jakoukoliv IP adresu počítače s Messaging Serverem spojeny s konkrétním NEWS serverem v Internetu.

```
192.168.1.0      255.255.255.0      0.0.0.0:news      news_srv.xyz.cz:news
```

Omezení přístupu určitých uživatelů k Internetu

Autentifikace do Proxy

Pokud hodláte omezit přístup jednotlivých uživatelů k Internetu pomocí jména a hesla, vyberte v konfiguraci Messaging Serveru službu Proxy a v nastavení zaškrtněte volbu Autentifikace požadována. Po restartu komunikačního serveru bude třeba pro přístup k Internetu nejprve zadat jméno a heslo.

Navíc máte možnost v Administrátorovi ve vlastnostech uživatele nastavit právo na použití Proxy. Kdo toto právo nemá, nedostane se browserem přes Proxy na Internet ani po zadání svého správného jména a hesla.

Zakázané URL

Existuje i možnost zakázat přístup na konkrétní adresy na Internetu z konkrétních počítačů. To lze provést pomocí nastavení „Zakázaných URL“ v Messaging Serveru v nastavení služby Proxy.

Konfigurační karta umožňuje omezení přístupu uživatelů proxy, SOCKS a DNS na zde specifikované servery, resp. zakazuje převod těchto URL na IP adresy. Uživatelé (stanice v síti), kterým má být zakázán přístup na danou URL adresu, se specifikují pomocí IP adresy a IP masky. Je tedy možné zakázat uvedené URL jen pro jeden počítač, nebo pro celou podsít' apod. Na rozdíl od IP filtru se zde zakázané cílové počítače specifikují svými jmény nebo jejich částmi doplněnými znaky „* a ?“.

Příklady

www.pornosoft.com ... zakáže přístup na jediný server konkrétního uvedeného jména

kachny ... zakáže přístup na všechny servery, v jejichž názvu se vyskytuje řetězec “kachny”

www.ufo.* ... zakáže přístup na počítač ve všech doménách/zemích (tj. například v doménách com, cz, sk atd.).

Seznam zakázaných URL lze vyexportovat do textového souboru nebo ho lze naopak z textového souboru načíst. Textový soubor musí obsahovat pouze takové řetězce, které obsahují URL adresy (na jednom řádku vždy jedna adresa). Na řádku také mohou být tři položky oddělené mezerami; první dvě položky jsou vstupní adresa a maska, třetí položkou je vlastní URL adresa – podobně jako na konfigurační kartě.

Nastavení IP filtru

Pomocí IP filtru můžete definovat, která spojení prostřednictvím proxy a SOCKS se mohou navazovat.

Pozn. Speciální IP filtry se dále používají i pro filtrování požadavků na SMTP server, a pro přístup k WWW serveru, který je součástí Mail602 Messaging Serveru. Tyto filtry se nastavují v konfiguraci příslušných služeb.

V sekci uprostřed karty vytvoříte seznam sítí a stanic, jimž (a na něž) je povolen nebo zakázán přístup. Jednotlivé položky se vkládají zápisem do čtveřice vstupních polí a stiskem tlačítka Přidat. Do polí Vstupní IP adresa a Vstupní maska zapište adresu a masku počítače nebo sítě, který požadavek vyslal. Do polí Cílová IP adresa a Cílová maska pak adresu a masku počítače, kam požadavek míří. Ke každé položce IP filtru je třeba definovat, zda znamená zákaz nebo povolení. K tomu je vlevo pod seznamem volič s dvojicí semaforů – červená znamená (podle očekávání) zákaz přístupu, zelená přístup povoluje.

Zopakování základních pojmů

Počítačová síť je definována IP adresou a maskou. IP adresa definuje hodnotu adres v síti, maska velikost sítě, tj. max. počet IP adres v dané síti. Pomocí bitové operace AND je pak možné např. zjistit, zda určitá konkrétní IP adresa patří do určité sítě.

Příklady masek :

255.255.255.255 ... jednotlivec; počítač s výše danou IP adresou,

255.255.255.0 ... všechny počítače dané sítě typu C (tj. prakticky 254 počítačů),

255.255.255.224 ... podsíť s 32 adresami (tj. prakticky 30 počítačů),

0.0.0.0 ... maska zahrnující všechny IP adresy, tedy celý Internet.

Princip činnosti IP filtru

Pomocí IP filtru se tedy ověřuje, zda je povoleno navázat určité spojení mezi dvěma počítači v Internetu. Vezme se tedy IP adresa počítače, který chce spojení navázat (KDO_IP) a adresa počítače kam se chce spojit (KAM_IP) a **postupně se procházejí položky IP filtru ve směru ze shora dolů** a hledá se, zda je dané spojení některou z položek zakázané (= záporný výsledek IP filtru) nebo zda je dané spojení povolené (= kladný výsledek IP filtru). Pokud se nenašla žádná odpovídající položka, je výsledek IP filtru též záporný. To umožňuje provést např. takové nastavení, které lokálním uživatelům zpřístupňuje celý Internet a přitom nejprve specifikovat jednotlivé počítače nebo sítě, kam přístup povolen není. Pokud je výsledek IP filtru kladný, může se dané spojení začít navazovat.

Zda se tedy daná položka IP filtru na dané spojení vztahuje, se zjišťuje podle následujících pravidel:

VSTUPNI_IP AND VSTUPNI_MASKA = KDO_IP AND VSTUPNI_MASKA

VYSTUPNI_IP AND VYSTUPNI_MASKA = KAM_IP AND VYSTUPNI_MASKA

Pokud chcete určitou položku seznamu zrušit, nastavte na ni ukazatel a stiskněte tlačítko Vymazat. Položku pod ukazatelem můžete také editovat, protože její obsah se přeneso do editačních okének.

Upozornění

Při použití dvoustupňové cache nelze v IP filtru používat omezení cílovou IP maskou, protože proxy server v tomto případě nezjišťuje IP adresu cílového počítače. Pro omezení přístupu k některým počítačům můžete použít filtr zakázaných URL.

Příklady nastavení IP filtru

- Všichni uživatelé sítě 192.168.1.0 mají mít možnost komunikovat s libovolným počítačem Internetu. Přitom z Internetu nemá být tato síť dosažitelná. Adresy nastavte na hodnoty:

| semafor | Vstupní adr. | Vstupní maska | Cílová adr. | Cílová maska |
|---------|--------------|---------------|-------------|--------------|
| zelená | 192.168.1.0 | 255.255.255.0 | 0.0.0.0 | 0.0.0.0 |

- Je třeba zajistit, aby všichni uživatelé lokální sítě s adresami 192.168.1.0 (s max. 255 počítači) mohli kamkoliv do Internetu, kromě serveru 194.196.5.193. Ostatní uživatelé z Internetu nebudou mít povoleno žádné spojení.

| semafor | Vstupní adr. | Vstupní maska | Cílová adr. | Cílová maska |
|---------|--------------|---------------|---------------|-----------------|
| červená | 192.168.1.0 | 255.255.255.0 | 194.196.5.193 | 255.255.255.255 |
| zelená | 192.168.1.0 | 255.255.255.0 | 0.0.0.0 | 0.0.0.0 |

- Je zapotřebí potlačit funkci IP filtru; spojení tedy bude možné mezi libovolnými počítači. Adresy nastavte v tomto případě na hodnoty:

| semafor | Vstupní adr. | Vstupní maska | Cílová adr. | Cílová maska |
|---------|--------------|---------------|-------------|--------------|
| zelená | 0.0.0.0 | 0.0.0.0 | 0.0.0.0 | 0.0.0.0 |

- Budete chtít povolit komunikaci pouze uživateli s IP 192.168.1.1. Adresy nastavte takto:

| semafor | Vstupní adr. | Vstupní maska | Cílová adr. | Cílová maska |
|---------|--------------|-----------------|-------------|--------------|
| zelená | 192.168.1.1 | 255.255.255.255 | 0.0.0.0 | 0.0.0.0 |

Konfigurace WWW serveru

Messaging Server

V konfiguraci Messaging Serveru přidejte službu WWW. Na záložce SSL WWW server máte poté možnost si v Nastavení SSL jednoduše stiskem tlačítka vytvořit soukromý a veřejný klíč pro zabezpečenou komunikaci mezi browserem a Vaším WWW serverem. Tu využijete zejména při přístupu do pošty pomocí browseru resp. WWW klienta.

Na kartě (SSL) WWW server lze nastavit adresáře pro práci WWW serveru.

Pokud chcete omezit přístup k WWW serveru (např. vytvořit jen vnitrofiremní Intranet), zapněte a nastavte IP filtr pro přístup k WWW serveru.

Na záložce Zprávy lze zapnout zaznamenávání operací prováděných WWW serverem i ve formátu W3C, čehož lze využít pro následnou analýzu některým z komerčně dostupných programů.

Pozn. Služba WWW je zapotřebí pro přístup do pošty z browseru (WWW klient) i pro přístup do pošty pomocí mobilního telefonu (WAP klient).

Administrátor – uživatelské WWW stránky

Ve stromu Uživatelé přejděte na položku Uživatelé WWW, kde ve složce WWWServer0 (resp. WWWServer1 pro SSL WWW server) můžete jednotlivým uživatelům založit jejich domovské adresáře a vygenerovat základ osobní stránky. Po stisku pravého tlačítka myši můžete změnit Základní adresář (hlavní adresář na disku s domovskými stránkami) a u jednotlivých uživatelů volbou Upravit nadefinovat jejich konkrétní domovský adresář – zadává se pouze název adresáře bez cesty (např. karel). Domovské stránky jsou pak browserem dostupné na adrese např. <http://server/~karel> (kde server je buď IP adresa počítače s Messaging Serverem nebo jeho platný název).

Administrátor – virtuální adresáře a přístupová práva

V programu Administrátor lze též definovat přístupová práva uživatelů do virtuálních adresářů WWW serveru (tzv. directory alias). Děje se tak ve stromu Uživatelé – Uživatelé WWW, ve složce WWWServer0 (resp. WWWServer1 pro SSL WWW server).

Ve stromu Virtuální adresáře je třeba zadat jméno tohoto virtuálního adresáře a reálný adresář, ve kterém jsou umístěny dané HTML soubory. Lze také zvolit zda se v tomto adresáři mohou spouštět CGI skripty a případně jméno autentifikace. Pro přístup do virtuálního adresáře z browseru je třeba zadat URL adresu ve tvaru <http://server/virtuálníadresář>. Pokud byla přiřazena autentifikace, bude třeba v browseru zadat nejprve jméno a heslo.

Seznam Autentifikací umožňuje definovat skupiny uživatelů, kteří mají mít přístup k určité oblasti WWW serveru (virtuálnímu adresáři). Při zakládání nové “autentifikace” zvolíme její jméno (např. Dealeri) a následně přes pravé tlačítko myši přidáme ze seznamu příslušné uživatele. Pro přístup může uživatel používat své heslo pro přístup do Mail602 nebo heslo zadané speciálně pro tuto autentifikaci.

Konfigurace faxování (nastavení služby Fax)

Administrátor

Při faxování z programů Mail602 Klient nebo Microsoft Outlook 9x/2000 (MAPI) lze k odesílaným faxům přidávat úvodní stránku včetně loga firmy, přičemž logo může být různé podle jazyka použitého ve faxu. Logo v různých grafických formátech lze zavést v pravé části okna po kliknutí na název poštovního úřadu. Odesílání faxů lze také časově omezit výběrem položky „Faxové spojení“.

Všechny došlé faxy jsou standardně doručovány do složky „Neroztříděné faxy“, do které mají přístup pouze uživatelé s právem „Rozdělování nezařazené pošty“, které jde nastavit ve vlastnostech jednotlivých uživatelů. Tato složka je dostupná všemi klientskými programy vyjma POP3 a WAP (viz Důležité poznámky k instalaci).

Faxy mohou být také doručovány přímo do došlé pošty konkrétním uživatelům na základě „identifikace“ odesílatěho faxu nebo ve spolupráci s pobočkovou ústřednou (viz dále), pokud mají nadefinována tzv. virtuální faxová čísla. V rámci Administrátora se toto nastavení provádí ve vlastnostech uživatelů na kartě „Adresy a čísla“ – Faxové číslo. Lze použít i zástupné znaky jako je * (hvězdička) a ? (otazník).

Messaging Server

V konfiguraci Messaging Serveru vyberte/přidejte službu Fax. Při přidávání ze seznamu zařízení, která jsou k dispozici, vyberte Vámi používaný faxmodem, který máte nainstalovaný ve Windows (např. TAPI-ZyXEL U-1496E ...) nebo přímo některý z komunikačních portů (např. COM2), na který máte faxmodem připojený.

Pozn. ISDN zařízení musí mít ve Windows nainstalované ovladače CAPI.

Pokud budete používat faxmodemy dva, přidejte službu dvakrát. Potom máte možnost v nastavení příslušné služby na první záložce říci, zda bude daný faxmodem určen pouze pro odesílání (pouze výstupní) nebo jen pro příjem faxů (pouze vstupní). Pokud ne zvolíte ani jednu z možností budou faxy odesílány či přijímány právě volným faxmodemem.

V nastavení služby fax proveďte následující úpravy :

- na záložce Zařízení zvolte dole záložku Pro odborníky a zvolte místo (a případně upravte jeho vlastnosti) v Pravidlech pro vytáčení – toto nastavení mj. ovlivňuje vytáčení tónovou/pulsní volbou nebo nuly pro státní linku atp.,
- při použití ISDN nastavte na příslušné záložce telefonní číslo, na kterém bude faxový server naslouchat (lze obvykle vybrat jedno ze čtyř telefonních čísel),

- na záložce FAX si můžete nastavit Identifikaci faxu, tj. text, který se zobrazuje protější straně při faxování.

Na záložce FAX lze také nechat všechny přijaté faxy automaticky tisknout na libovolné tiskárně, která je z daného počítače (ve Windows) s komunikačním serverem. Faxy se tisknout okamžitě po dokončení jejich příjmu komunikačním serverem.

Informace o nalezené OLE podpoře Vás informují, jaké soubory můžete připojit k odesílanému faxu a komunikační server je automaticky zkonvertuje do faxového formátu.

Při potížích s odesíláním či příjmem faxů zkuste snížit rychlosti vysílání/příjmu na dolní záložce FaxModem na záložce FAX, případně nastavte ovládací příkazy manuálně na Class1.

Nastavení pobočkové ústředny

Pro přímé doručování faxů konkrétním uživatelům do jejich poštovních schránek, je třeba jim nastavit v Administrátorovi virtuální faxová čísla a dále nastavit ústřednu tak, aby volání na tato čísla směřovala na linku s faxmodemem připojeným k Messaging Serveru. Po přijetí volání faxmodemem mu musí být ústředna schopna zopakovat tónově (DTMF volbou) původně volané číslo (linku). Pokud ústředna při opakování čísla vkládá před/za něj nějaké další znaky, nastavte v Administrátorovi číslo se zástupnými znaky „?“ (např. pokud ústředna pro číslo 123 předává AA123B, pak nastavte ??123?).

Konfigurace telefonního záznamníku

Administrátor

Po přihlášení k poštovnímu úřadu klikněte na jeho název a v pravé části okna nastavte položku „Uvítací zpráva pro modemy“ podle typu Vašeho faxmodemu. Pokud si nejste typem modemu jisti, vyzkoušejte Rockwell (příp. HCF Rockwell).

Hlasové vzkazy jsou standardně doručovány do složky „Nezařaditelná pošta“, do které mají přístup pouze uživatelé s právem „Rozdělování nezařazené pošty“, které jde nastavit ve vlastnostech jednotlivých uživatelů.

Hlasové vzkazy také mohou být ve spolupráci s pobočkovou ústřednou doručovány přímo do došlé pošty konkrétním uživatelům (viz dále), pokud mají nadefinována tzv. hlasová čísla, která většinou bývají shodná s linkovým číslem daného uživatele. V rámci Administrátora se toto nastavení provádí ve vlastnostech uživatelů na kartě „Adresy a čísla“ – Hlasové číslo. Lze použít i zástupné znaky jako * (hvězdička) a ? (otazník).

Vzdálené ovládání telefonního záznamníku

Pokud uživatelé ve vlastnostech povolíte Hlasový přístup a na záložce „Jména a hesla“ mu nastavíte heslo pro hlasový přístup (heslo nesmí obsahovat jiné znaky než číslice), bude mít možnost pracovat s nahranými vzkazy i vzdáleně pomocí libovolného telefonu s tónovou volbou.

Stačí, když zavolá na telefonní číslo, kde naslouchá komunikační server a po vyzvednutí linky zadá tónově číslo své linky (svoje „Hlasové číslo“) a následně své „hlasové“ heslo.

Dále je možno používat tyto povely :

- 1 přehraj zprávy (implicitní)
- 2 přehraj předchozí zprávu
- 4 přehraj jen neviděné/resp. všechny
- 5 smaž aktuální zprávu/resp. (po dokončení přehrávání všech zpráv) smaž všechny zprávy
- 6 další zprávu
- 7 (po dokončení přehrávání všech zpráv), konec=polož linku
- 0 přeskoč všechny zprávy
- * přeskoč uvítací zprávy
- 99zaznamenej novou vlastní uvítací zprávu
- # potvrzení nové vlastní uvítací zprávy

Messaging Server

V konfiguraci Messaging Serveru přidejte službu Hlas (pokud ještě není v seznamu aktivních služeb) a ze seznamu zařízení, která jsou k dispozici, vyberte Vámi používaný modem s podporou hlasu (voice), který máte nainstalovaný ve Windows (např. TAPI-ZyXEL U-1496E ...) nebo přímo některý z komunikačních portů (např. COM2), ke kterému je modem připojen.

V nastavení služby na kartě Hlas vyberte Hlasový mód odpovídající typu Vašeho modemu (pokud si nejste jisti, vyzkoušejte typ Rockwell nebo HCF Rockwell).

Nastavení pobočkové ústředny

Pro přímé doručování hlasových vzkazů konkrétním uživatelům do jejich poštovních schránek, je třeba jim nastavit v Administrátorovi hlasová čísla a dále nastavit ústřednu tak, aby pokud volaný uživatel do určitého počtu zazvonění (nebo do určité doby) nezvedne telefon, směřovala volání na linku s faxmodemem připojeným k Messaging Serveru. Po přijetí volání faxmodemem mu musí být ústředna schopna zopakovat tónově (DTMF volbou)

původně volané číslo (linku). Pokud ústředna při opakování čísla vkládá před/za něj nějaké další znaky, nastavte v Administrátorovi číslo se zástupnými znaky „?“ (např. pokud ústředna pro číslo 123 předává BB123A, pak nastavte ??123?).

Zpřístupnění informací o uživateli (nastavení LDAP)

Administrátor

Po přihlášení k poštovnímu úřadu klikněte na jeho název a v pravé části okna zvolte „Údaje pro LDAP server“ a vyberte, jaké informace budete navenek o uživateli poskytovat. Tato nastavení se dotkne pouze uživatelů, které Administrátor povolil zobrazovat pomocí LDAP serveru.

Ve vlastnostech konkrétního uživatele nejprve na kartě „Práva a přístup“ zaškrtněte „Zobrazovat údaje v LDAP serveru“. Následně vyplňte informace na kartě LDAP (zobrazeny budou pouze údaje označené symbolem „X“).

Messaging Server

V konfiguraci Messaging Serveru přidejte službu LDAP (pokud ještě není v seznamu aktivních služeb). Jméno a heslo pro administrátorský přístup do LDAP serveru se týká aplikací třetích stran, které mohou zapisovat údaje přímo do LDAP serveru.

Konfigurace odesílání a příjmu SMS

Varianta – odesílání i příjem

Pokud potřebujete, aby odesílání krátkých textových zpráv (SMS) bylo spolehlivější a byl umožněn i jejich příjem, přidejte v konfiguraci Messaging Serveru službu SMS a jako zařízení zvolte GSM telefon připojený k serveru. V nastavení služby je třeba ještě na kartě SMS vyplnit číslo servisního centra mobilního operátora, případně i PIN telefonu.

V Administrátorovi lze pak jednotlivým uživatelům nastavit jejich privátní „SMS čísla“ (může to být i řetězec znaků). Pokud příchozí SMS obsahuje jako první slovo toto „SMS číslo“, je automaticky doručena přímo do schránky příslušného uživatele.

Konfigurace spojení Mail602

Pro přenos zásilek mezi Mail602 poštovními úřady (nebo mezi programem Mail602 Klient a komunikačním serverem) se používá šifrovaný protokol Mail602 s možností komprimace vyvinutý přímo pro toto použití. Vyznačuje se dobrým systémem šifrování

(standard, DES - zejména při spojení úřadů přes heslo) a schopností navázání přenosu dat po předchozím předčasném rozpojení přenosu.

Tento protokol je možné použít na řadě přenosových médií, především se jedná o modemy (AT příkazy), ISDN (CAPI rozhraní), TCP/IP (po LAN nebo i s vytáčením).

Administrátor

Nastavení parametrů vlastního úřadu

Nejprve je vhodné změnit implicitní nastavení týkající se vlastního poštovního úřadu. To lze učinit v hlavní konfiguraci po kliknutí na název poštovního úřadu.

Nastavení se provádí na záložkách dle typu spojení. Zatímco u telefonního spojení se na dolní záložce nastavují tel. čísla, u TCP/IP spojení se nastavují IP adresy. Je možno nastavit až 8 čísel (adres). U telefonního čísla se vždy určuje, zda se jedná o standardní analogovou linku nebo o ISDN (X.75 nebo V.120). Další parametry jsou shodné pro oba typy spojení.

Je vhodné vybrat **exportní seznam**, který se bude při daném typu spojení implicitně přenášet na protější úřad. Dále je vhodné nastavit maximální čekací dobu (případně i počet zásilek), po které budou zásilky odeslány. V opačném případě budou zásilky odesílány okamžitě po zařazení do výstupní fronty. Samozřejmě, že lze také časově omezit jak příjem, tak i odesílání zásilek (graficky myší nebo pomocí menu kliknutím pravým tlačítkem).

Přístup pouze přes heslo zabezpečuje poštovní úřad před navázáním spojení se zcela neznámými poštovními úřady. Pokud použijete tuto volbu, nezapomeňte toto heslo nastavit o tři řádky níže.

Automatická výměna zásilek zajišťuje, že při spojení jsou odeslány zásilky pro protější úřad a zároveň jsou přijaty zásilky pro vlastní úřad.

Potvrzování zásilek umožňuje mezi úřady přenášet doručky, tzn. odesílat potvrzení o přečtení doporučených zásilek.

Při **automatické výměně seznamů** se mezi poštovními úřady automaticky přenášejí aktualizované exportní seznamy, tj. seznamy dostupných adresátů na příslušném úřadě.

Navázání spojení s externím poštovním úřadem

Pokud chcete navázat spojení s nějakým externím Mail602 poštovním úřadem, přejděte do stromu Připojení a zvolte Protější úřady. Po kliknutí pravým tlačítkem myši v pravé části okna zvolte Nový.

Většina parametrů se nastavuje analogicky s předchozím tématem (jako u vlastního úřadu) s tím rozdílem, že se navíc zadává např. tel. číslo (IP adresa) protějšního úřadu.

Pozn. 1 Na kartě **Domény** uvede administrátor tohoto úřadu poštovní domény nebo internetové adresy, které akceptuje tento úřad pro doručování zásilek s internetovými adresami přímo na protějšní úřad spojením Mail602. Kromě přímého vyjmenování domén je také povolen znak *. Zadáním hvězdičky ovšem snižujete bezpečnost, protože pokud protějšní úřad pošle seznam, ve kterém bude uvedena adresa ve skutečnosti ležící v Internetu, dojde k přenosu zásilek na protějšní úřad místo do Internetu.

Jinými slovy : Při komunikaci mezi dvěma poštovními úřady verze 4 (a vyplněnou kartou Domény/Adresy) se tedy do výstupní fronty zásilek vkládají zásilky v internetovém formátu a až komunikační server na základě porovnání domén/adres rozhodne, zda se zásilka bude přenášet pomocí SMTP nebo pomocí Mail602 kódovaného spojení. Pokud karta Domény/Adresy zůstane prázdná, uživatelé budou mít k dispozici pouze Mail602 adresy a budou tedy posílat zásilky ve starém Mail602 formátu. Obsah nabízeného seznamu je zobrazen v kartě Došlý seznam.

Pozn. 2 V řádku **Specifikace serverů** je možné vybrat službu Messaging Serveru, která se bude spojovat s tímto protějšním úřadem. Čísla služeb jsou zobrazena v konfiguraci Messaging Serveru na kartě Komunikační služby jako jejich ID. Do této řádky v Administrátoru se zapisuje pouze číselná hodnota. Pokud je odpovídajících služeb více, oddělují se čárkami.

Příklad: pokud se má na tento úřad volat pouze modemy obsluhovanými službami ID03 a ID05, zapíšeme do specifikace serverů čísla "3,5".

Princip zálohování spojení

V případě, že pro protějšní úřad zvolíte oba typy spojení (telefonní i TCP/IP), pak v jeho vlastnostech můžete určit, který druh spojení bude preferován pro prvních „x“ pokusů. Pokud se spojení nepodaří po „x“ pokusech navázat, začne se zkoušet alternativní spojení.

Např. Pětkrát se zkusí spojení po TCP/IP a pokud se nepovede navázat, dojde k pokusu o navázání přímého modemového spojení (třeba po ISDN).

Exportní seznamy

Pomocí exportních seznamů může administrátor definovat, jací uživatelé mají být „nabízeni“ ke komunikaci protějšním Mail602 poštovním úřadům. Exportních seznamů lze založit několik a používat je dle potřeby – např. v jednom budou uvedeni pouze obchodní

zástupci pro Čechy a ve druhém jen pro Slovensko. Pro komunikaci s partnery na Slovensku pak administrátor nastaví seznam obsahující pouze obchodní zástupce ze Slovenska.

Telefonický a TCP/IP přístup programem Mail602 Klient

Pokud má mít uživatel možnost přistupovat k poště programem Mail602 Klient protokolem TCP/IP nebo modemem, je třeba mu v jeho vlastnostech povolit „TCP/IP a Telefonní přístup“. Další nastavení se provádí po rozbalení stromu Připojení. Je třeba nastavit parametry pro „Tel. a TCP/IP přístup“.

Položka exportní seznam specifikuje seznam lokálních uživatelů (může být i upravený), který bude mít klient při tel/TCP přístupu k dispozici.

Pro zvýšení bezpečnosti poštovního úřadu lze říci, že při tel/TCP přístupu bude nejprve ověřeno heslo pro přístup k poštovnímu úřadu, a teprve pak se bude ověřovat jméno a heslo uživatele.

Uživatele přistupujícího po tel/TCP lze omezit maximální velikostí odesílaných resp. přijímaných zásilek a také časově – kdy nemůže služeb poštovního úřadu/serveru využívat.

Messaging Server

Službu Mail602 lze při přidávání klasicky přiřadit buď k protokolu TCP/IP nebo k modemu (CAPI ISDN, TAPI zařízení, COM port). Je také možno mít službu přidanou dvakrát (jednou pro TCP/IP a podruhé pro modem), čehož se využívá při zálohování spojení.

Ve vlastnostech služby Mail602 lze na záložce Služba specifikovat používanou úroveň šifrování při přenosu a pracovní intervaly. Také lze specifikovat, zda mají být zásilky při přenosu komprimovány.

Při použití ISDN nezapomeňte na stejnojmenné záložce zadat telefonní číslo, na kterém bude server „naslouchat“.

Konfigurace NT/2000 služby

Na Windows NT/2000 lze Messaging Server provozovat jako službu.

Ve Windows založte uživatele (např. mail602); v jeho vlastnostech odškrtněte volbu „Při dalším přihlášení uživatel musí změnit heslo“ a naopak zaškrtněte volbu „Heslo je platné stále“. Tohoto uživatele přiřadte do skupiny Administrators.

Messaging Server

Instalace služby se provádí v „Konfiguraci pro odborníky“ na záložce „NT služba“. Tuto službu je třeba spouštět pod UŽIVATELSKÝM účtem (např. mail602 – viz výše), neboť

systemový účet nemá přístup k síťovým cestám ani neumí pracovat s cestami v UNC formátu (\\server\cesta). Jako parametr příkazové řádky uveďte cestu na poštovní úřad (\\počítač\sdílení\cesta). V části okna „Službu startovat až po ...“ zaškrtněte Browser (Computer Browser).

Pozn. Pokud chcete měnit konfiguraci Messaging Serveru běžícího jako služba, spusťte Messaging Server pomocí upraveného zástupce s parametrem „/config“ přidaným na konec řádku Cíl nebo použijte vzdálenou správu browserem.

Vzdálená správa

Messaging Server (správa přes web)

Kromě přímé administrace na konzoli je možné Messaging Server spravovat vzdáleně pomocí browseru, a to jak z počítače na lokální síti tak z internetu. V konfiguraci pro odborníky na záložce Administrace lze povolit dálkové ovládání komunikačního serveru tzn. konfigurace, sledování provozu, navazování dial-up atd.

Pokud chcete zabezpečit přístup do konfigurace z menu v okně Messaging Server, zaškrtněte volbu **Omezit přístup ke konfiguraci přímo z programu pouze na administrátory**. Pak bude při každém pokusu o vstup do Konfigurace pro odborníky i do Průvodce konfigurací vyžadováno zadání jména a hesla uživatele s administrátorskými právy.

Vzdálená administrace pomocí browseru

Parametry související se správou Messaging Server se nastavují na záložce **Administrace**. Vzdálenou administraci pomocí browseru povolíte zaškrtnutím volby **Povolit dálkové ovládání pomocí browseru**. Vzdálená administrace je pak dostupná na adrese <http://adresaserveru/admin>.

V sekci **Přihlášení ke vzdálenému ovládání** můžete upřesnit míru zabezpečení vzdálené administrace:

- **žádné – volný vstup** – do vzdálené administrace bude mít přístup kdokoliv!
- **vyžadováno přihlášení uživatele** – pro vstup bude třeba zadat uživatelské jméno a heslo libovolného uživatele Messaging Server
- **přístup pouze pro administrátory** – vstup do vzdálené administrace budou mít pouze uživatelé Messaging Server s právy administrátora (*doporučujeme*).

Použití zvláštního portu nebo SSL

Implicitně je vzdálené ovládání a administrace součástí web serveru (je spuštěno na stejném portu a nachází se ve virtuálním adresáři /ADMIN). Z bezpečnostních důvodů je možné vzdálené ovládání a administraci přesunout na jiný port a případně vyžadovat použití zabezpečeného protokolu HTTPS.

Po zaškrtnutí volby **Použít zvláštní port pro vzdálené ovládání** zadejte číslo portu, na kterém chcete vzdálené ovládání provozovat (např. 8081).

Pokud požadujete, aby se ke vzdálenému ovládání dalo připojit pouze pomocí zabezpečeného protokolu HTTPS, zaškrtněte i volbu **Použít SSL protokol**.

Poznámka: Na jakou adresu je třeba se připojit pro přístup k vzdálené administraci ukazuje dynamicky text psaný kurzívou umístěný pod těmito volbami.

Update obsahu WWW serveru pomocí FTP

Stránky jsou na WWW serveru uloženy v adresářích definovaných na záložce **WWW** v konfiguraci Messaging Server. Jejich aktualizaci lze provádět nejen přímou prací se soubory na disku (standardně v podadresáři **DOCS**), ale i vzdáleně pomocí protokolů HTTP a FTP.

Aktualizaci obsahu WWW serveru pomocí protokolu FTP povolíte zaškrtnutím volby **Povolit FTP update WWW serveru na portu X** (standardně 21). Toto nastavení neovlivní možnost provádět update stránek pomocí protokolu HTTP.

Pozn. Pokud potřebujete na počítači s Messaging Server provozovat jiný FTP server, změňte hodnotu portu (např. na 8021).

Další zabezpečení vzdálené administrace

Pro zvýšení bezpečnosti můžete přístup ke vzdálené administraci i FTP update obsahu WWW serveru omezit navíc pomocí speciálního IP filtru zaškrtnutím volby **Pro přístup k dálkovému ovládání a FTP update platí IP filtr**, který lze nastavit po stisku tlačítka **IP filtr dálkového ovládání a FTP update**.

Např. přístup ke vzdálené administraci a FTP update pouze v rámci Vaší lokální sítě povolíte zpravidla zadáním IP adresy 192.168.1.1 a masky 255.255.255.0 (přístup bude povolen ze všech počítačů s IP adresou 192.168.1.x).

Poštovní úřad (správa pomocí DCOM)

Pokud splňuje Vaše instalace potřebné předpoklady (viz Důležité poznámky k instalaci), můžete celý poštovní úřad spravovat vzdáleně pomocí stejného uživatelského rozhraní.

Na počítači, ze kterého chcete poštovní úřad spravovat, (nainstalujte a) spusťte program Administrátor. Klikněte pravým tlačítkem na text u ikonky Administrátor a zvolte přidat počítač. Zadejte IP adresu administračního serveru a vyčkejte připojení. Přihlášení a správa zvoleného poštovního úřadu pak již probíhá naprosto shodně s „lokální“ administrací.

Pozn. Na klientském počítači je třeba být přihlášen jako uživatel, který existuje i na administračním serveru a je tam ve Windows členem skupiny Administrátoři.

Konfigurace modelu DCOM pro použití administrační služby

Následující popis je určen pro speciální případy instalace, kdy je Administrátor nainstalován na administračním serveru jako služba.

PŘI KLASICKÉ INSTALACI TOTO NASTAVENÍ NEPROVÁDĚJTE !

- 1) Na administračním serveru spusťte manuálně program *dcomcnfg.exe* (součást Windows),
- 2) zvolte vlastnosti u položky „Mail602 Administrator DCOM server“,
- 3) nastavte položku „Úroveň ověřování“ na „žádné“ (část Obecné),
- 4) nastavte „Spouštět v tomto počítači“ (část Umístění),
- 5) nastavte „Vlastní oprávnění“ (část Zabezpečení) a přidejte do seznamu uživatele, pod jehož účtem běží Messaging Server jako služba, a povolte mu plné ovládání,
- 6) V konfiguraci modelu DCOM nastavte ve výchozích vlastnostech žádné/anonymní ověřování a zaškrtněte oba checkboxy (DCOM i COM Internet).

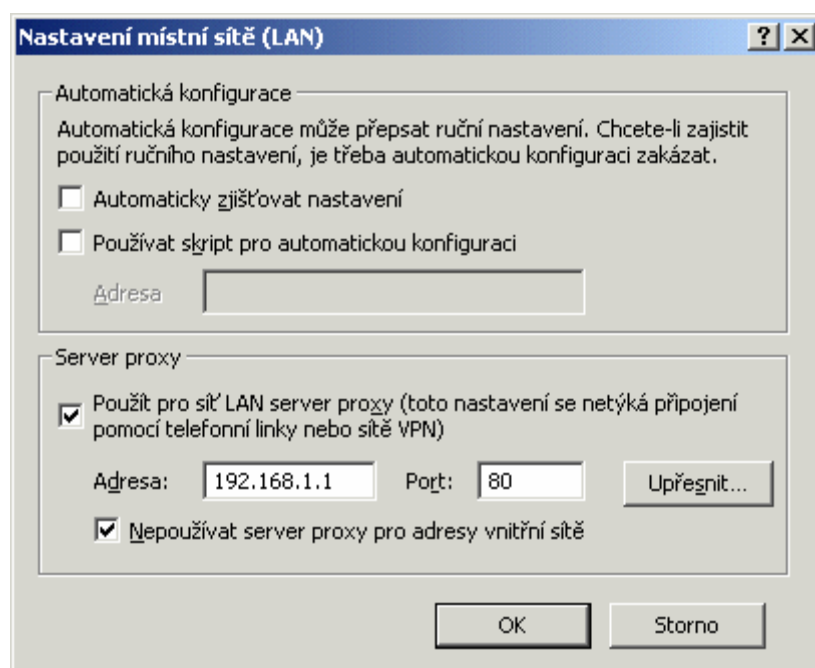
Klientské programy

- **Mail602** – přístup pomocí programu Mail602 Klient po lokální síti, protokolem TCP/IP (i přes Internet) nebo přímo modem-modem,
- **POP3** – např. MS Outlook Express, Netscape Messenger,
- **MAPI** – přístup z MS Outlook 9x/2000,
- **WWW/WAP** – přístup do pošty z browseru/mobilního telefonu.

Nastavení internetového prohlížeče

V případě, že máte nakonfigurován NAT, nemusíte žádné nastavení aplikace Internet Explorer provádět. Na druhou stranu je používání proxy výhodné, neboť umožňuje administrátorům lepší kontrolu nad chováním jednotlivých uživatelů.

- 1) Spustíte Internet Explorer.
- 2) V menu vyberte **Nástroje, Možnosti internetu ...**,
- 3) klikněte na záložku **Připojení**,
- 4) stiskněte **Nastavení místní sítě**,
- 5) zaškrtněte **Použít pro síť LAN server proxy** a vyplňte IP adresu počítače s Messaging Server (např. 192.168.1.1) a port 80. Zaškrtněte také **Nepoužívat server proxy pro adresy vnitřní sítě**. Ujistěte se, že nejsou zaškrtnuty žádné volby v sekci Automatická konfigurace.



- 6) Potvrzujte **OK**, dokud se nevrátíte na základní obrazovku browseru.

Elektronický podpis a šifrování zásilek (S-MIME)

Abyste mohli začít využívat technologie S-MIME pro elektronické podepisování a/nebo šifrování zásilek, musíte nejprve získat tzv. certifikát (nebo také Digital ID), který obsahuje Vaš veřejný klíč certifikovaný nějakou certifikační autoritou.

Jak získat certifikát

Pro získání certifikátu je třeba o něj nejprve zažádat na www stránkách certifikační autority (u nás např. na www.ica.cz). Při podávání žádosti vygeneruje browser unikátní dvojici klíčů – soukromý a veřejný, načež veřejný předá certifikační autoritě k certifikaci. Ta po ověření totožnosti (v případě testovacích certifikátů bez ověření) vydá žadateli certifikát.

Žádost o certifikát a jeho následnou instalaci je vhodné provádět z browseru, se kterým „spolupracuje“ klientský program pro práci s poštou, jenž hodláte v budoucnu používat. V opačném případě je nutno klíč nejprve vyexportovat a následně naimportovat do příslušného browseru.

Do kterého browseru certifikát instalovat a jak certifikát vyexportovat se dozvíte v následujících odstavcích.

Důležitá upozornění

Soukromý klíč je vygenerován a uložen na počítači, ze kterého byla podána žádost o certifikát. Navíc je dostupný pouze tomu uživateli, který ho vygeneroval. Certifikát je svázán s e-mailovou adresou. V případě její změny je nutno žádat o nový certifikát. Pokud chcete certifikát a soukromý klíč přenést na jiný počítač, je třeba ho nejprve vyexportovat.

Doporučujeme Vám si certifikát včetně soukromého klíče vyexportovat a zálohovat na bezpečné místo, neboť v případě jeho ztráty či poškození (např. při porušení instalace Windows) si nebudete moci Vám (i dříve) doručené zašifrované e-maily přečíst !

Je třeba zajistit maximální možnou ochranu soukromého klíče, tj. zabezpečit přístup ke klíči i do Windows heslem (příp. i do počítače) atp.

Internet Explorer a správa certifikátů

Instalaci certifikátu do Internet Exploreru je třeba provést v případě, že chcete používat některý z následujících poštovních programů :

- Mail602 Klient,
- MS Outlook Express,
- MS Outlook 98/2000.

Export certifikátu včetně soukromého klíče je dostupný posloupností Nastavení – Možnosti sítě Internet – záložka Obsah – Certifikáty – po výběru tlačítka Exportovat.

Netscape Communicator a správa certifikátů

Instalaci certifikátu do Netscape Communicatoru je třeba provést v případě, že chcete pro práci s elektronickou poštou využívat Netscape Messenger, který je jeho součástí.

Export certifikátu včetně soukromého klíče je dostupný posloupností Communicator – Tools – Security Info – položka Yours pod Certificates – po výběru tlačítka Export.

Jak odeslat elektronicky podepsanou a/nebo zašifrovanou zprávu

Než začnete posílat elektronicky podepsané či zašifrované zprávy, je třeba nastavit Vámi používaný klientský program – viz následující odstavce.

Pokud chcete někomu poslat elektronicky podepsanou zprávu, stačí pak v klientském programu zvolit (stisknout tlačítka) elektronicky (digitálně) podepsat (někdy také parametr Signed) a zprávu odeslat.

Pokud chcete, aby byla zpráva i zašifrovaná a její obsah nemohl rozšifrovat nikdo jiný než její oprávněný příjemce, zvolte „Zašifrovat“. To můžete ale udělat až poté, co získáte certifikát adresáta Vaší zprávy a přiřadíte ho k odpovídající adrese v seznamu adresátů. Pokud tedy ještě tento certifikát nemáte, nechte si od Vašeho korespondenčního partnera poslat elektronicky podepsanou zprávu, ve které je certifikát automaticky obsažen.

Nastavení Mail602 Klient

V menu Nastavení vyberte Nastavení prostředí Mail602 Klienta a zvolte záložku Bezpečnost. Z nabídky aliasů vyberte e-mailovou adresu, k níž hodláte získaný certifikát přiřadit, a stiskněte tlačítka Vybrat. Ze seznamu certifikátů vyberte ten, který chcete používat. Dále můžete upravit upřednostňovaný šifrovací algoritmus, a také kdy Vás má program upozornit, že úroveň šifrování použitá v nějaké zprávě je příliš nízká (nebezpečně).

Z důvodu zachování kompatibility se staršími klientskými programy při posílání elektronicky podepsaných zpráv doporučujeme zaškrtnout volbu Používat oddělený podpis.

Pokud si chcete uložit adresu odesílatele elektronicky podepsané zprávy spolu s jeho certifikátem tak, abyste mu mohli příště poslat zašifrovanou zprávu, vyberte Vlastnosti zprávy a po volbě Uložit adresu odesílatele přiřaďte k adrese tlačítkem Vybrat z nabídnutého seznamu příslušný certifikát. Pak již můžete adresu uložit do libovolného seznamu.

Nastavení Outlook Express

V aplikaci Outlook Express není třeba provádět žádná nastavení. Při prvním pokusu o odeslání elektronicky podepsané zprávy budete pouze vyzváni k potvrzení certifikátu (Digital ID), který chcete používat. Vše ostatní již aplikace nastaví automaticky za Vás.

Nastavení MS Outlook 9x/2000

V menu Nástroje zvolte Možnosti a záložku Zabezpečení. Po stisku tlačítka nastavit zabezpečenou el. poštu zadejte nějaký název (formát ponechte S/MIME). Zaškrtněte obě volby o výchozím nastavení a tlačítkem vybrat vyberte Podpisové osvědčení (Osvědčení zašifrování se vyplní automaticky.). Ponechte zaškrtnutou volbu o posílání těchto osvědčení se zabezpečenými zprávami.

Nastavení Netscape Messenger

Netscape Communicator je nastaven pro posílání elektronicky podepsaných a/nebo šifrovaných zásilek automaticky po instalaci certifikátu.

Mail602 Klient

Existují dva základní typy instalace programu Mail602 Klient :

- uživatelský,
- administrátorský.

Uživatelská instalace programu Mail602 Klient

Slouží k instalaci programu Mail602 Klient na lokální pevný disk na počítači v síti.

- Instalace se spouští z adresáře MESSAG\MAIL602\USER\Disk1.
- Po spuštění stačí zadat identifikační údaje (jméno a firmu), zvolit cílový adresář.

Administrátorská instalace programu Mail602 Klient

Instalace se spouští z adresáře MESSAG\MAIL602\NETINST\Disk1. Instaluje program Mail602 Klient na síť, přičemž lze volit ze dvou možností. Po spuštění administrátorské instalace, budete moci po zadání identifikačních údajů a cílového adresáře zvolit jednu ze dvou možností :

- **Kopírování instalačních souborů** – výsledkem je pouze **kopie** instalačních souborů na síťovém disku, která obsahuje předvolené typy přístupů k poště. Uživatelé pak

mohou instalovat program Mail602 Klient na svůj lokální disk ze sítě. Každý uživatel má tedy na konec program na svém lokálním disku.

- **Instalování síťové instalace** – provede instalaci programu Mail602 Klient na síťový disk, odkud potom program spouští uživatelé. Nejprve ale musí ze síťového adresáře spustit setup.exe, který jim vytvoří ikony, tiskárnu Fax602 a zaregistruje aplikaci.. Program je tedy nainstalován pouze na síťovém disku a uživatelé u sebe mají pouze konfigurační soubory.

Ovládání programu Mail602 Klient

Ovládání programu Mail602 Klient je intuitivní a podobá se ovládání ostatních programů pro práci s elektronickou poštou. Na tomto místě proto zmíníme pouze několik zajímavých funkcí.

Koncepty (rozepsané dopisy)

Každý vytvářený dopis můžete kdykoliv v průběhu práce uložit jako tzv. koncept. Takto můžete uložit libovolný počet dopisů a kdykoliv se k nim později vrátit, dokončit je a odeslat. Koncept můžete uložit pomocí příslušné ikony nebo při zavírání okna s editorem. Všechny uložené koncepty naleznete ve složce **Koncepty**.

Dopis se také může ukládat jako koncept **automaticky v pravidelných intervalech**, pokud toto nastavíte na záložce Editor v menu Nastavení – Nastavení prostředí Mail602 Klienta.

Pokud chcete, aby se koncept po odeslání dopisu odstranil, zaškrtněte volbu **mazat koncepty po odeslání**. Tu naleznete na záložce Odesílání v menu Nastavení – Nastavení prostředí Mail602 Klienta.

HTML editor

Pro přípravu dopisu se standardně používá prostý textový editor, který neumožňuje např. používat tučné či barevné písmo nebo do textu vkládat obrázky. Pokud chcete vytvářet takto formátované dopisy, zapněte na záložce Editor v menu Nastavení – Nastavení prostředí Mail602 Klienta volbu **Pro přípravu dopisu použít HTML editor**.

Mazání zásilek do koše

Zásilky, které vymažete, mohou být před svým fyzickým odstraněním nejprve přesunuty do Koše, odkud je můžete v případě potřeby bez problémů obnovit. Tuto funkci můžete

kdykoliv zapnout nebo vypnout pomocí volby **při mazání zásilek používat koš**, kterou naleznete na záložce Obecné v menu Nastavení – Nastavení prostředí Mail602 Klienta.

Pozn. Tato funkce nijak neovlivňuje ani nesouvisí s nastavením archivace zásilek, které může měnit pouze administrátor poštovního úřadu.

Automatické mazání zásilek z přihrádek

Pokud kliknete pravým tlačítkem myši na přihrádku založenou pod složkou Došlá pošta nebo na Koš, budete mít po výběru **Nastavení automatického mazání...** možnost určit, po jaké době budou zásilky z dané přihrádky automaticky odstraněny. To může být výhodné u složky Koš, pokud používáte mazání zásilek do Koše nebo třeba u přihrádky, do které jsou tříděny spamy.

Nastavení vzhledu a nástrojových lišt

Mail602 Klient obsahuje několik témat (barevných schémat) pro zobrazení. Můžete si je vybírat z menu **Použít téma pro zobrazení**, které naleznete na záložce Zobrazení v menu Nastavení – Nastavení prostředí Mail602 Klienta.

Velikost ikon zobrazovaných na nástrojových lištách můžete ovlivnit volbou **použít malé ikony**, kterou naleznete rovněž na záložce Zobrazení.

Jaké ikony budou zobrazeny můžete ovlivnit kliknutím pravým tlačítkem na jednotlivé zobrazené nástrojové lišty a volbou **Konfigurace**.

Učení bayesovského antispamového filtru

Uživatel může došlou nevyžádanou zasilku označit jako **Spam** pomocí příslušné ikony na nástrojové liště nebo z kontextového menu dostupného pravým tlačítkem myši. Pokud je označeno více zásilek v seznamu, budou všechny označeny jako spam a server se je v závislosti na konfiguraci naučí. Analogicky může uživatel označovat „legální“ zasilky jako **Nespam**.

V závislosti na nastavení může také uživatel manuálně přidávat odesilatele zásilek na svoji černou nebo bílou listinu.

Nastavení antispam

V tomto nastavení, které je dostupné přes menu Nastavení – Nastavení prostředí Mail602 Klienta – záložka Antispam, může uživatel podrobněji specifikovat, jak mají být označovány a zpracovávány zasilky označené jako nevyžádané (spam). Dále je zde informován o centrálním nastavení bayesovského filtru, které provedl administrátor.

Metoda testování

Pokud uživatel zaškrtně volbu **Používat bílou a černou listinu**, budou doručované zprávy kromě centrálního bayesovského filtru porovnávány ještě s těmito „listinami“ a v případě výskytu odesílatele na černé listině označeny jako spam.

Odesílatelé zpráv označených uživatelem jako **Spam** budou automaticky přidáváni na černou listinu, zatímco odesílatelé zpráv označených uživatelem jako **Nesпам** budou přidáváni na bílou listinu, pokud bude zaškrtnuta volba **Sloučené ovládání antispam funkcí**. Pokud tato volba zatržena není, objeví se v uživatelském rozhraní kromě tlačítek spam/nesпам navíc tlačítka pro zápis adresy odesílatele na černou resp. bílou listinu.

Označení spamu

Pokud administrátor nezapnul centrální bayesovský filtr a neprovedl tedy nastavení centrálně, může zde uživatel specifikovat, jak mají být označovány nevyžádané zprávy na základě výskytu odesílatele na černé listině.

Akce se spamem

Zpráva označená jako spam může být:

- přesunuta do přihrádky (síťově nebo lokální)
- odstraněna – zpráva je nenávratně vymazána

Bílá a černá listina

Bílá listina obsahuje seznam adres odesílatelů, jejichž zprávy nebudou nikdy považovány za spam. **Černá listina** obsahuje seznam adres odesílatelů, jejichž zprávy budou vždy považovány za spam. Obsah bílé i černé listiny lze také importovat a exportovat ve formátu TXT.

Pozn. Toto nastavení je uživatelské, a proto zprávy označené jako spam na základě výskytu jejich odesílatele na černé listině jsou zpracovávány až na základě nastavení uživatele v sekci **Akce se spamem** a nikoliv podle centrálního nastavení v Messaging Server.

POP3 klient

Hlavní výhodou použití POP3 klienta (např. MS Outlook Express) je to, že je zdarma součástí operačního systému Windows a uživatelé ho zpravidla používají i doma pro práci se svou soukromou elektronickou poštou.

Obecný SMTP/POP3 poštovní klient

Pro práci s elektronickou poštou v rámci Messaging Server můžete použít libovolný poštovní klientský program podporující protokol SMTP/POP3.

Pro odesílání pošty je třeba nastavit adresu SMTP serveru jako IP adresu počítače s Messaging Server (např. 192.168.1.1) a zadat vlastní e-mailovou adresu uživatel@doména dle konfigurace Messaging Server (např. karel4@firma.cz).

Pro příjem pošty je třeba nastavit adresu POP3 serveru jako IP adresu počítače s Messaging Server (např. 192.168.1.1), případně zvolit typ serveru POP3. Dále je třeba zadat přihlašovací jméno (název účtu) a heslo – odpovídá jménu uživatele a heslu v Messaging Server.

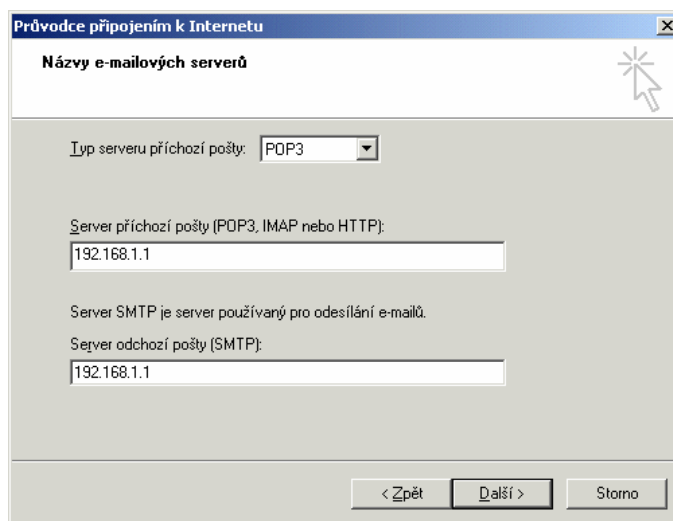
Učení bayesovského antispamového filtru

Bayesovský filtr mohou učit uživatelé ve svém SMTP/POP3 klientském programu (např. Outlook Express) prostřednictvím přeposílání nevyžádaných zásilek (spamů) na adresu spam@spam a vyžádaných (normálních) zásilek na adresu notspam@spam.

Outlook Express

Postup nastavení programu Outlook Express pro spolupráci s Messaging Server.

- 1) Spustíte Outlook Express. Postupujte podle průvodce nebo z menu **Nástroje** vyberte **Účty – Přidat – Pošta...**
- 2) Do řádku **Zobrazované jméno** vyplňte Vaše plné jméno a klikněte na **Další**.
- 3) Vyberte, že již máte e-mailovou adresu a vyplňte ji do řádku **E-mailová adresa** a klikněte na **Další**.



- 4) Typ serveru příchozí pošty nastavte na **POP3** a **Server příchozí pošty** i **Server odchozí pošty** nastavte na IP adresu počítače s Messaging Server (např. 192.168.1.1) a klikněte na **Další**.
- 5) Nyní vyplňte **Název účtu** (uživatelské jméno v Messaging Server) a **Heslo** (stejně jako v Messaging Server) a klikněte na **Další**.
- 6) Stiskněte tlačítko **Dokončit**.

Jak faxovat z POP3 klienta ?

Uživatelé POP3 klientských programů (např. MS Outlook Express, Netscape Messenger, apod.) mohou odesílat faxy v zásadě dvěma způsoby :

- odesláním e-mailu na adresu ve formátu číslo@fax,
- tiskem na tiskový ovladač Fax602, který je součástí instalace programu SendFax.

Zkontrolujte si také nastavení Messaging Serveru a Administrátora, která souvisejí s POP3 klienty – viz výše.

Faxování přímo z SMTP/POP3 poštovního klienta

Fax lze napsat a odeslat přímo a jednoduše jako standardní e-mail na adresu ve formátu číslo@fax (např. 222011218@fax). Messaging Server obsah dopisu převede na fax a odešle ho na číslo, které je součástí adresy. Převod faxu včetně souborů připojených k záznamu probíhá pomocí vnitřních funkcí programu (většinou grafické formáty) nebo pomocí funkcí OLE automation voláním asociovaných aplikací (např. MS Word pro formát DOC, atd.).

Pokud používáte MS Outlook Express nebo MS Outlook 9x/2000, můžete si faxová čísla zapisovat přímo do příslušných položek v Kontaktech (fax do zaměstnání, fax domů), a ty pak využít při posílání faxových zásilek. Tuto funkci je třeba povolit zaškrtnutím políčka v konfiguračním dialogu programu SendFax.

Tisk na tiskárnu Fax602 a nastavení programu SendFax

Druhý způsob faxování spočívá v tisku na virtuální tiskárnu-faxový ovladač, který je součástí instalace programu SendFax. Tak lze faxovat z libovolné Windows aplikace, která umožňuje volbu tiskárny. Pro faxování pak jen stačí nastavit jako tiskárnu Fax602 a po zvolení adresáta přímo z Adresáře Outlook Express je fax odeslán. Adresy lze volit také z adresářů poštovních programů podporujících standardní rozhraní MAPI (např. z Kontaktů v MS Outlooku 9x/2000) nebo Simple MAPI (např. Netscape Messenger).

Instalace programu SendFax se spouští z adresáře MESSAG\POP3\Disk1.

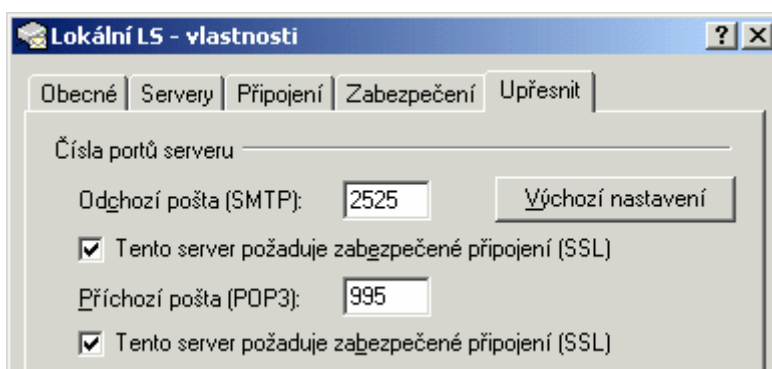
V programu SendFax je třeba nastavit tři (v některých případech čtyři) položky :

- **602Pro Server** – IP adresa počítače, na němž běží Messaging Server.
- **Vaše e-mail adresa** – zpravidla ta, kterou máte nastavenou v POP3 klientovi.
- **Seznamy** - program SendFax si neudrží vlastní seznamy faxových adresátů - ty je třeba udržovat v jednom z nabízených klientských programů - buď MS Outlook Express nebo některý MAPI klient, například MS Outlook 9x/2000, případně některý Simple MAPI klient (např. Netscape Messenger).
- **Automatická konverze faxových adres/zásilek** - Pokud používáte MS Outlook Express nebo MS Outlook 9x/2000, můžete si faxová čísla zapisovat přímo do příslušných položek v Kontaktech (fax do zaměstnání, fax domů), a ty pak využít při posílání faxových zásilek. Jinou možností je faxové číslo zadat do adresáře přímo jako standardní e-mail adresu ve formátu číslo@fax (např. 420-222011218@fax).

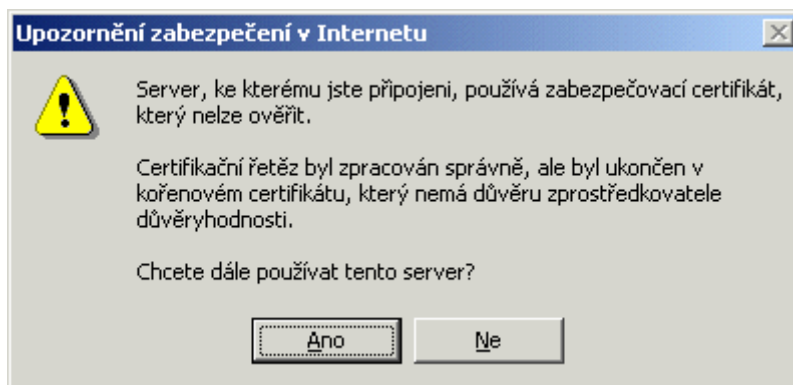
Nastavení Outlook Express pro SSL SMTP/POP3

Zabezpečení SMTP a POP3 serveru pomocí SSL zabraňuje mj. „odposlechu“ Vašeho hesla i Vašich e-mailů na cestě mezi SSL SMTP/POP3 serverem a Vaším počítačem. Pokud chcete, aby práce s Vaší POP3 schránkou a komunikace se SMTP serverem probíhala šifrovaně pomocí SSL, je třeba toto nastavit jak v Messaging Server, tak v klientském programu.

V programu **Outlook Express** je ještě třeba kromě standardního nastavení ve vlastnostech poštovního účtu na záložce **Upřesnit** zaškrtnout pod čísla portů pro SMTP i POP3 volby **Tento server požaduje zabezpečené připojení (SSL)**. Dále u SMTP přepsat číslo portu na **2525** a provedená nastavení potvrdit **OK**.



Pokud administrátor Messaging Server sám vygeneroval a podepsal SSL klíče, zobrazí se při přístupu z Outlooku Express k SSL SMTP/POP3 serveru následující hlášení:



Pozn. V aplikaci Mozilla Suite je zabezpečení SMTP prostřednictvím SSL (nikoliv TLS) podporováno od verze 1.7. Nezapomeňte zkontrolovat a případně upravit číslo portu.

Vyhledávání e-mailových adres a informací u uživatelích

Outlook Express

Zvolte v menu Nástroje – Účty a po stisku tlačítka Přidat vyberte Adresářová služba. Jako adresu LDAP serveru zadejte IP adresu počítače s Mail602 Messaging Serverem. Na závěr vyberte právě zadanou adresářovou službu a v jejích vlastnostech na kartě Upřesnit zadejte jako výchozí bod vyhledávání c=CZ.

Nyní můžete vyhledávat pomocí této služby např. e-mailové adresy volbou „Najít osoby“ buď v programu Outlook Express nebo přímo z Windows přes menu Start-Nají-Osoby.

Netscape Messenger

V menu Communicator zvolte Address Book. V okně Address Book vyberte v menu File – New Directory. Adresářovou službu si libovolně pojmenujte, do řádky LDAP server zadejte IP adresu počítače s Mail602 Messaging Serverem a do řádky Search Root zadejte c=CZ.

Pokud chcete pomocí této Adresářové služby vyhledávat klikněte na ni v levé části okna nebo si ji předvolte v konfiguraci programu.

MAPI klient (MS Outlook 9x/2000)

MAPI podporu je třeba nainstalovat na všechny stanice, ze kterých budou uživatelé přistupovat k poštovnímu úřadu systému Mail602 programy MS Outlook 9x/2000.

Instalace MAPI podpory

Před instalací MAPI podpory je třeba nastavit MS Outlook 9x/2000 jako výchozího poštovního klienta (zpravidla v nastavení Internet Exploreru na záložce Programy).

Instalace se spouští z adresáře MESSAG\MAPI\Disk1. Instalace probíhá automaticky a na jejím závěru se spustí průvodce nastavením profilu pro MS Outlook 9x/2000.

Z nabízených služeb vyberte Mail602 služby, a pak vyplňte název profilu. Následně zadejte „cestu na EMI“ (cestu k poštovnímu úřadu) a vyplňte jméno a heslo uživatele.

Vyberte si způsob zpracování zásilek a pokud hodláte používat pro práci s poštou pouze (většinou) MS Outlook 9x/2000, zaškrtněte příslušnou volbu. Tato dvě nastavení lze kdykoliv změnit z Ovládacích panelů volbou Pošta (Mail602 služby-Vlastnosti-karta Došlá pošta).

Doporučujeme ještě zkontrolovat nastavení ukládání osobních adres. Nastavení lze provést opět přes Ovládací panely volbou Pošta na záložce Adresy. Je třeba mít nastaven konkrétní vlastní adresář nebo Kontakty.

Přístup k poště a nastavením systému Mail602

Pro nastavení parametrů a funkcí systému Mail602 je po instalaci MAPI podpory v Outlooku dostupná nová záložka Mail602 v menu Nastavení-Možnosti.

Zde lze mj. nastavit automatické třídění došlé pošty – odpovědi, postupování, SMS avíza na mobilní telefon apod.

Složky systému Mail602 (Došlá pošta, Archiv, Fronty zásilek, atd.) se zobrazí v seznamu složek, který lze buď zobrazit trvale přes menu Zobrazit nebo jen dočasně kliknutím na název otevřené složky (např. Doručená pošta).

Poznámky

Pokud chcete zadat ručně adresáta faxu, zadejte do elektronické adresy faxové číslo a jako typ el. adresy vyplňte FAX602.

Pro ruční odeslání SMS zprávy zadejte telefonní číslo a jak typ el. pošty vyplňte SMS.

WWW klient

Nejjednodušší a zároveň nejuniverzálnější způsob pro práci s poštou v systému Mail602 představuje WWW Klient, pro jehož používání stačí mít nainstalovaný pouze browser (např. Internet Explorer).

Pro vyvolání WWW klienta stačí do browseru zadat URL ve tvaru `http://server/mail` nebo pro přístup zabezpečený pomocí SSL pak `https://server/mail` (kde server je buď IP adresa počítače s Messaging Serverem nebo jeho název). Po zadání jména a hesla lze již normálně pracovat s poštou.

Upozornění : Při úplně prvním vyvolání WWW klienta je třeba zadat kromě jména a hesla i cestu k poštovnímu úřadu (nejlépe ve tvaru `\\server\cesta`).

Pozn. : WWW klient je součástí instalace komunikačního serveru.

WAP klient

Do pošty lze přistupovat i z mobilních telefonů podporujících protokol WAP. Pomocí WAP klienta lze provádět základní operace s poštou, jako je odesílání nové a čtení, odpovídání a mazání došlé pošty.

WAP klient je přístupný po zadání cesty `http://server/wap` do prohlížeče v mobilním telefonu. Po zadání přihlašovacího jména a hesla se uživateli zobrazí seznam jeho došlé pošty. Další operace se provádějí výběrem ze zobrazeného menu. Některé užitečné funkce WAP klienta lze najít i v menu „Options“, jehož způsob vyvolání je závislý na typu používaného telefonu (spec. tlačítko u tel. Nokia, přidržené tlačítko Yes u tel. Ericsson, apod.).

Pozn. Pro využívání WAP klienta je třeba, aby byla v rámci Messaging Serveru zprovozněna služba WWW a aby byl tento server přímo přístupný z Internetu. Rovněž je třeba uskutečnit nejprve alespoň jeden přístup z WWW klienta, při kterém dojde k zadání cesty k poštovnímu úřadu.

Pozn. : WAP klient je součástí instalace komunikačního serveru.

Systémové požadavky

Pro provoz Mail602 MESSAGING SERVER doporučujeme počítač s procesorem řady Pentium s alespoň 128 MB paměti RAM, operačním systémem Windows 2000/2003/XP a Microsoft Internet Explorer 6.

Minimální požadavky na server

Operační systém: Mail602 MESSAGING SERVER vyžaduje jeden z následujících OS:

- Windows 98/ME (přečtěte si Důležité poznámky)
- Windows NT 4.0 + SP5 + MSIE 5.5
- Windows 2000/2003/XP

Processor: Pentium a vyšší

Paměť: minimální velikost paměti závisí na používaném OS

- 32 MB RAM - Windows 98/ME
- 64 MB RAM - Windows NT/2000/XP
- 128 MB RAM - Windows 2003

Prostor na disku: 40 MB + další prostor dle využívání pošty, proxy cache atd.

Důležité poznámky

1. Firewall a překlad adres (NAT) funguje pouze pokud je komunikační server provozován na počítači s operačním systémem Microsoft Windows 2000/2003/XP.
2. Provoz Mail602 MESSAGING SERVER vyžaduje na počítači nainstalovaný minimálně Microsoft Internet Explorer 5.5 a vyšší.
3. NEDOPORUČUJEME použití Windows 98/ME jako operačního systému na serveru v sítích s více než 10 stanicemi.
4. Pošta (zásilky, archiv) může být uložena i na jiném file serveru (např. Novell Netware)

Minimální požadavky na stanice

- hardware odpovídající použitému operačnímu systému
- operační systém dle používaného klientského programu:
- browser nebo POP3 klient - libovolný systém s podporou TCP/IP
- MAPI nebo Mail602 klient - Windows 9x/NT/2000/2003/XP
- místo na disku pro program Mail602 Klient přibližně 18 MB

- Mail602 Klient vyžaduje nainstalovaný MS Internet Explorer 5.5 a vyšší.