

ALWIL Software

avast32

MS SMTP 2000 Server Edition

Obsah

1	Úvod	5
2	Instalace	7
2.1	Požadavky na vybavení počítače	7
2.2	Instalujeme	8
3	První kroky	9
4	Konfigurace rezidentní úlohy	11
4.1	Stránka „Úloha“	11
4.2	Stránka „Typ“	12
4.3	Stránka „Rezidentní“	12
4.4	Stránka „MS SMTP 2000“	13
4.5	Stránka „Testování“	13
4.6	Stránka „Akce“	14
4.7	Stránka „Zprávy a logy“	15
4.8	Stránka „Upřesnit“	16
4.9	Stránka „Plánování“	18
5	Použití Avastu pro MS SMTP Server	19
5.1	Instalace při použití v režimu e-mail gateway	19
5.2	Instalace při použití v MS Exchange 2000	21
5.3	Používání notifikací	22
5.4	Používání krátkých textů na konec zpráv	24
5.5	Další vhodná nastavení Avastu	25

Seznam obrázků

4.1	Stránka „Úloha“	11
4.2	Stránka „Typ“	12
4.3	Stránka „Rezidentní“	12
4.4	Stránka „MS SMTP 2000“	13
4.5	Stránka „Testování“	13
4.6	Stránka „Akce“	14
4.7	Stránka „Zprávy a logy“	15
4.8	Stránka „Upřesnit“	16
4.9	Okno „Nastavit tabulku lokálních odesílatelů“	17
4.10	Okno „Nastavit tabulku lokálních adres“	18
4.11	Stránka „Plánování“	18
5.1		20
5.2	Implicitní notifikace, kterou Avast posílá odesílateli zavirované zprávy	22

1 Úvod

Vážený zákazníku, blahopřejeme Vám k zakoupení antivirového prostředku AVAST32 3.0, SMTP Server Edition (popř. Avast32, Exchange Server Edition), jednoho z nejlepších programů ve své třídě. Doufáme, že budete s našim produktem spokojeni a že se Vám s ním bude příjemně pracovat.

AVAST32 3.0 SMTP Server Edition představuje úplnou antivirovou ochranu pro poštovní provoz na bázi protokolu SMTP ve Vaší organizaci. Pracuje jako plugin do SMTP služby, jež je standardní součástí každé instalace Windows 2000/XP (workstation i server). Tento plugin lze použít i v případě, že Váš poštovní server pracuje na zcela jiné architektuře (např. OS UNIX/Linux). Podrobné informace o tom, jak chránit nehomogenní prostředí tohoto druhu naleznete v dalších kapitolách.

Kromě toho modul Avast32, SMTP Server Edition funguje i jako plugin do MS Exchange 2000 Serveru, takže jej lze jednoduše použít i pro ochranu SMTP provozu na poštovních serverech založených na Exchange 2000.

V případě jakýchkoli problémů s programem či nejasností kontaktujte svého prodejce nebo firmu ALWIL Trade. Jejich pracovníci Vám rádi a ochotně poradí.

Příjemnou a viry nerušenou práci na Vašem počítači Vám přejí pracovníci firmy ALWIL Software.

2 Instalace

AVAST32 pro SMTP Server 2000 je nová verze antivirového systému AVAST vytvořeného speciálně jako plugin do služby MS SMTP Server, která je standardní součástí Windows 2000/XP (není-li nainstalována, je možno ji kdykoli doinstalovat z Ovládacích panelů, Přidat/ubrat programy). Je dodáván jako součást antivirové suity Avast32, Exchange Server Edition (to proto, že ji lze použít jako plugin do Exchange 2000) a též tvoří cenově výhodnější produkt Avast32, SMTP Server Edition. Jádro programu je určeno pro počítač s Windows 2000/XP Workstation nebo Serverem nebo MS Exchange 2000 Serverem. Konfiguraci ale můžete provádět z jakékoli síťové stanice s Windows 95/98 nebo Windows NT4/2000/XP. Program se skládá ze dvou částí:

- první je serverová, která provádí samotné testování a která je nainstalována přímo na počítač, na kterém běží MS SMTP 2000 Server (Service), nebo MS Exchange 2000
- druhá je klientská, což je vlastně jenom přídatný modul do běžné instalace programu AVAST32 verze 3.0, který Vám umožní vzdálenou administraci serverové části.

AVAST32, SMTP2000/Exchange Server Edition vyžaduje, abyste již měli nainstalován AVAST32 verze 3.0. Před započítím instalace se ujistěte, že je AVAST32 verze 3.0 instalován, a to jak na serveru, tak na klientské stanici, ze které budete chtít provádět správu (nejedná-li se o samotný server).

2.1 Požadavky na vybavení počítače

K tomu, aby mohl být AVAST32 úspěšně nainstalován na Váš počítač a poté i bezchybně pracovat, je nutné, aby Váš počítačový systém splňoval několik základních požadavků.

Pro instalaci serverové části:

- procesor Pentium nebo vyšší
- 32 MB paměti RAM
- Windows 2000 nebo XP Workstation nebo Server
- V systému nainstalovaná komponenta SMTP Service nebo Exchange 2000 Server

Poznámka: zda použít OS workstation nebo server závisí hlavně na Vás. Podle vyjádření Microsoftu Vám ale stačí na provozování Avastu, který bude chránit SMTP pro celou síť, *jediná klientská licence*. Zároveň ale určitě doporučujeme, aby kde-li o ochranu velké sítě (více než několik set mailboxů) byl Avast provozován na serverovém OS, a to zejména kvůli jeho vyšší stabilitě, robustnosti a škálovatelnosti (která se podle vyjádření Microsoftu liší i pro samotnou SMTP službu).

Pro instalaci jako klient

- počítač splňující požadavky na běh programu AVAST32 verze 3.0

2.2 Instalujeme

Jak již bylo řečeno, serverovou část můžete provozovat buďto na počítači s nainstalovaným MS SMTP Serverem, nebo na počítači s MS Exchange 2000. První případ se používá většinou tehdy, kdy počítač s Avastem slouží jakási SMTP gateway, jejímž účelem je hledat viry (samozřejmě, můžete používat i MS SMTP Server sám o sobě (jako hlavní poštovní server), ale to je spíše výjimka). Pro obecný postup instalace v tomto případě viz sekce Instalace při použití v režimu e-mail gateway. Instalujete-li naopak na Exchange 2000 Server, je pro Vás určena sekce Instalace při použití v MS Exchange 2000.

<To be supplied>

3 První kroky

Po úspěšně dokončené instalaci a restartu Windows můžete ihned nové funkce programu AVAST32 začít používat.

Veškeré funkce AVAST32 3.0 SMTP Server Edition jsou ovládány prostřednictvím úlohy, vytvořené v rozšířeném ovládní programu AVAST32 3.0.

Pro spuštění programu AVAST32 klikněte na tlačítko „Start“, pak zvolte složku „Programy“, dále nalistujte složku „AVAST32 Antivirus“ a v této složce klikněte na ikonu „AVAST32“.

Po spuštění programu se ujistěte, zda pracujete v rozšířeném ovládní. Pokud pracujete v jednoduchém ovládní klikněte levým tlačítkem myši na ikonu v levém horním rohu programu a vyberte rozšířené ovládní ze zobrazeného menu.

Podrobný popis vytváření úloh pro ochranu SMTP 2000 Serveru se nachází v následujících kapitolách.

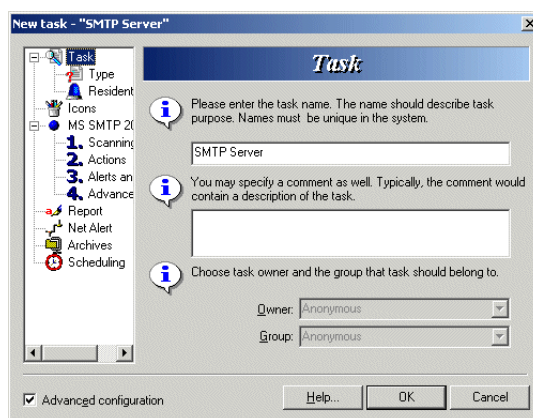
4 Konfigurace rezidentní úlohy

V následujícím textu budou popsány jednotlivé stránky s ovládacími prvky, které se týkají nastavení úlohy na rezidentní ochranu MS SMTP Serveru 2000 (popřípadě SMTP provozu na Exchange 2000). Obrázky zobrazené u jednotlivých stránek ukazují stránky při použití stromu při konfiguraci úlohy. Při použití průvodce nebo záložkového seznamu je podoba okna jiná, ale ovládací prvky a jejich význam jsou však tytéž.

Pro rezidentní ochranu můžete použít jak standardní úlohu „Rezidentní ochrana“ (po příslušné modifikaci, popsané níže - konkrétně zahrnutí poskytovatele „MS SMTP 2000“), tak i zcela novou, vámi definovanou úlohu. Tu vytvoříte následujícím postupem: na stránce „Úlohy“ rozšířeného ovládacího panelu klikněte pravým tlačítkem myši na seznamu úloh nebo klikněte na nabídku „Úloha“ v hlavním menu programu, a ze zobrazeného menu vyberte položku „Vytvořit novou ...“. Zobrazí se dialog pro vytvoření nové úlohy.

4.1 Stránka „Úloha“

Na stránce „Úloha“ (obr. 4.1) je programem požadováno vložení jména vytvářené úlohy. To by mělo být co možná nejvýstižnější a nemělo by být kvůli přehlednosti shodné s některým jménem již existující úlohy. Jestliže nezadáte žádné jméno, nebude nová úloha vytvořena. Implicitně textové pole obsahuje „(nespecifikováno)“.



4.1 Stránka „Úloha“

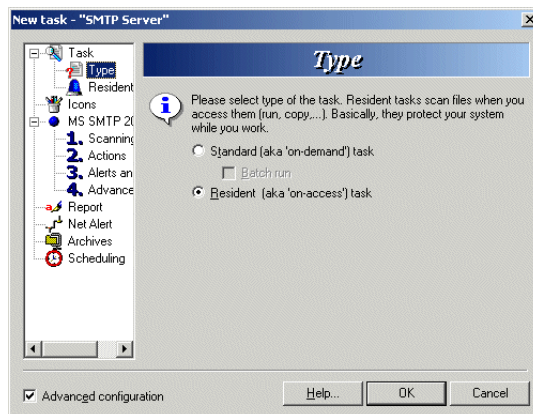
Do dalšího textového pole je možné napsat komentář úlohy stručně popisující činnost úlohy. Tato položka může zůstat prázdná.

Pomocí kombinovaného pole „Skupina“ nastavte skupinu, do které úloha patří.

Pomocí kombinovaného pole „Vlastník“ nastavte vlastníka, kterému úloha patří.

4.2 Stránka „Typ“

Na stránce „Typ“ (obr. 4.2) zvolte pomocí přepínače „Rezidentní“ vytváření rezidentní úlohy

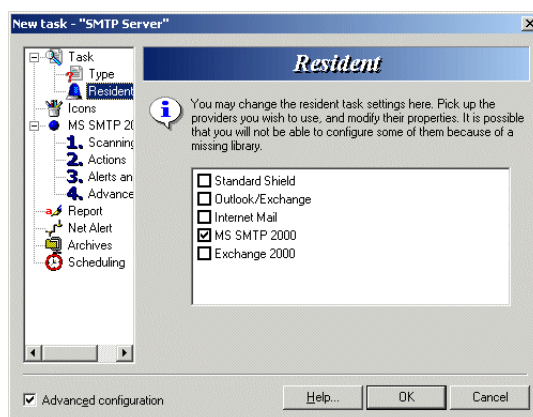


4.2 Stránka „Typ“

Po zvolení přepínače se automaticky změní možnosti dalšího nastavení úlohy.

4.3 Stránka „Rezidentní“

Stránka „Rezidentní“ (obr. 4.3) obsahuje seznam dostupných poskytovatelů rezidentní ochrany.



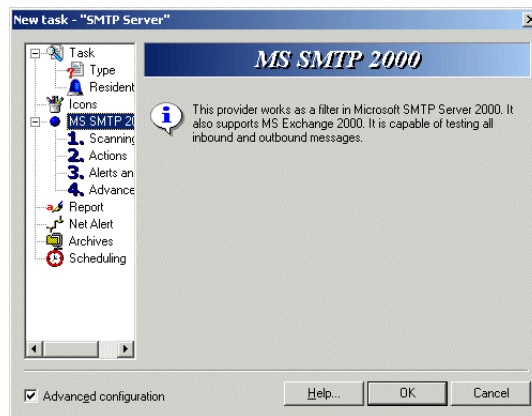
4.3 Stránka „Rezidentní“

Počet položek uvedených v seznamu je závislý na verzi programu, kterou používáte, a též na počtu instalovaných komponent. Na této stránce zaškrtněte zaškrťovací pole „MS SMTP 2000“. U ostatních položek seznamu můžete (ovšem nemusíte) zaškrtnutí zrušit, pokud nechcete dané poskytovatele používat. Například plně podporovaná konfigurace je i ta, kde na stejném počítači používáte jak poskytovatele pro MS SMTP 2000, tak i Standardní štít.

Jedinou výjimkou z tohoto pravidla je poskytovatel Internet Mail - jeho používání na serverech není doporučeno. Důvodem je skutečnost, že tento poskytovatel pro svou činnost používá jednoduchý SMTP/POP3 server. Protože pro tyto služby jsou přiděleny pevná čísla TCP portů (u SMTP jde o 25, v případě POP3 je to 110), je možné na jednom počítači provozovat nejvýše jeden takový server. Na serveru však pravděpodobně běží „opravdový“ SMTP server (v tomto případě patrně MS SMTP Service nebo Exchange 2000), takže by při použití poskytovatele Internet Mail docházelo ke kolizím při společném používání TCP portu.

4.4 Stránka „MS SMTP 2000“

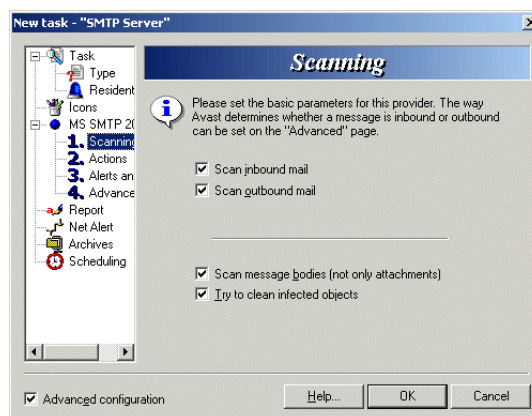
Tato stránka zobrazuje pouze informace o zvoleném poskytovateli rezidentní ochrany.



4.4 Stránka „MS SMTP 2000“

4.5 Stránka „Testování“

Stránka „Testování“ (obr. 4.5) umožňuje uživateli nastavit základní parametry poskytovatele.



4.5 Stránka „Testování“

Pomocí zaškrťovacího pole „Testovat příchozí zprávy“ určíte, že poskytovatel bude testovat zprávy pocházející zvenčí a doručované někomu na tomto serveru nebo uvnitř Vaší organizace.

Zaškrtnutím zaškrťovacího pole „Testovat odchozí zprávy“ zajistíte testování zpráv, které naopak pocházejí od někoho z Vaší organizace.

Jde-li o zprávu, kterou adresovala osoba A osobě B na tomtéž serveru (nebo uvnitř Vaší organizace), Avast ji považuje za odchozí (nejprve totiž ze serveru „odchází“).

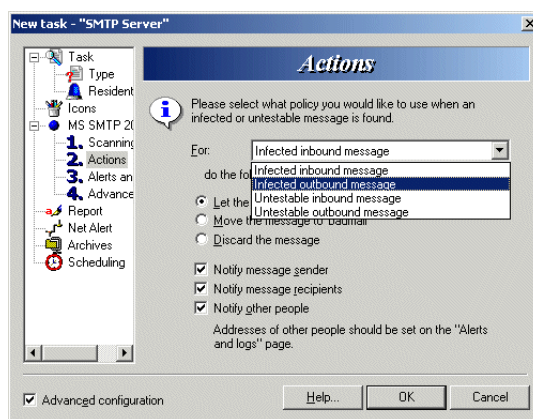
Podotkněme, že aby Avast mohl správně rozeznávat odchozí zprávy od příchozích, je třeba, aby byl korektně nastaven způsob, jak toto rozeznávání provádět, a rovněž volitelně další parametry, které se tohoto nastavení týkají. Toto nastavení se provádí na poslední konfigurační stránce poskytovatele MS SMTP 2000, Upřesnit.

Přepínačem „Testovat těla zpráv (tzn. nejen přílohy)“ se zapíná možnost testování těl zpráv, a to ve všech formátech (plain-text, HTML, RTF apod.). Vzhledem k tomu, že v současné době již existují viry, které se šíří v tělech zpráv (např. nechvalně známý BubbleBoy), je ve většině případů žádoucí mít tento parametr zapnut.

Konečně volba „Lze-li, odvirovávat infikované objekty“ určuje, zda se má Avast pokoušet čistit zavirované objekty, a lze-li je skutečně odvirovávat, jejich čistou verzi ke zprávě připojovat. Ve většině případů bývá tato volba zapnuta.

4.6 Stránka „Akce“

Stránka „Akce“ (obr. 4.6) umožňuje uživateli nastavit politiku, kterou bude Avast používat při jednotlivých krizových situacích. Konkrétně jde o případy nalezení infikované nebo netestovatelné odchozí nebo příchozí zprávy.



4.6 Stránka „Akce“

V poli „Pro“ si nejprve zvolíte, pro jakou situaci chcete nastavení provádět. K dispozici jsou následující volby, jejichž význam je zřejmý:

- Infikovaná příchozí zpráva
- Infikovaná odchozí zpráva
- Netestovatelná příchozí zpráva

- Netestovatelná příchozí zpráva

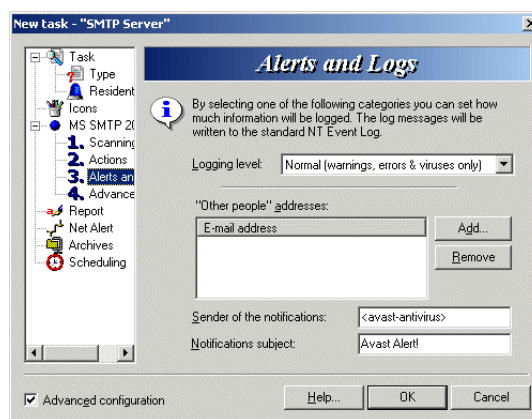
Ostatní pole tohoto okna nastavují akci, kterou Avast provede v případě, že nastane situace zvolená v poli „Pro“.

První nastavení tvoří skupina tří přepínačů, které určují, co má Avast se zprávou udělat. Zaškrtnutí pole „Umožnit doručení zprávy“ určuje, že Avast umožní normální zpracování infikovaných/netestovatelných zpráv, jako by tuto vlastnost neměly. Naproti tomu zvolíte-li „Přesunout zprávu do složky 'badmail'“ určujete tím, že Avast má takovéto zprávy automaticky přesouvat do složky s nedoručitelnou poštou (v případě MS SMTP 2000 služby jde o složku „Badmail“ v adresáři MailRoot). Poslední možností je volba pole „Smazat zprávu“, která způsobí, že všechny zprávy, splňující danou vlastnost, budou nepodmíněně smazány.

Druhá skupina polí se týká notifikací, které se budou posílat. K dispozici jsou notifikace pro odesílatele (volba „Notifikovat odesílatele zprávy“), příjemce (volba „Notifikovat příjemce zprávy“) a též libovolné další osoby (volba „Notifikovat další osoby“). Nastavení adres těchto dalších osob se provádí na konfigurační stránce „Zprávy a logy“.

4.7 Stránka „Zprávy a logy“

Na stránce „Zprávy a logy“ (obr. 4.7) je možné nastavit jednak úroveň, s jakou bude poskytovatel MS SMTP 2000 zapisovat logovací zprávy (užitečné zejména při řešení nej-různějších problémů) a též další parametry pro notifikační zprávy, jejichž posílání lze aktivovat na stránce „Akce“.



4.7 Stránka „Zprávy a logy“

Volba úrovně logování se provádí pomocí pole „Úroveň logování:“. K dispozici jsou čtyři úrovně:

- Maximální
- Vysoká
- Normální (pouze varování, chyby a viry)
- Nízká (pouze varování a chyby)

Maximální úroveň zapíná velmi důkladné logování. Doporučeno pouze při hledání příčin problémů, neboť může rychle vést k zaplnění logu. Vysoká úroveň vypouští některé

ze zpráv, zapisovaných na maximální úrovni, stejně však ponechává i množství zpráv, které mají spíše informativní charakter. Úroveň Normální (standardně nastavena) způsobuje, že logovat se budou pouze varování, chyby a zprávy o nalezení virů. Konečně úroveň Nízká se od Normální liší tím, že hlášení o nalezení viru nejsou do logu zaznamenávány.

Všechny zprávy se zapisují do aplikačního NT Event Logu.

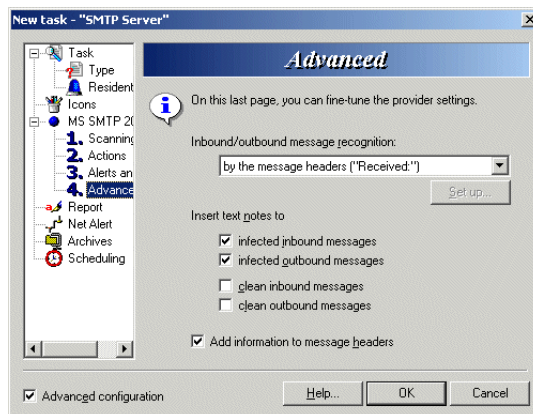
Další nastavení, která lze na stránce Zprávy a logy provést, se týkají notifikací. V poli „Adresy ostatních osob“ se nastavuje, komu se budou posílat dodatečné notifikaci o krizové situaci. Pro editaci seznamu použijte tlačítka „Přidat...“ a „Odstranit“. Do seznamu je záhodno zapsat např. adresy administrátorů. Adresy uvádějte v tradiční SMTP formě *jméno@doména*.

Pomocí pole „Odesílatel notifikací:“ můžete specifikovat adresu, která bude uvedena v RFC822 záhlaví *From:* všech notifikací, které bude Avast rozesílat. Uvedete-li platnou SMTP adresu (např. administrátora), bude možné na notifikace odpovídat.

Konečně pole „Předmět notifikací:“ určují předmět notifikačních zpráv (RFC822 záhlaví *Subject:*).

4.8 Stránka „Upřesnit“

Na stránce „Upřesnit“ (obr. 4.8) je možné doladit nastavení poskytovatele MS SMTP 2000.



4.8 Stránka „Upřesnit“

Pomocí pole „Způsob detekce příchozích/odchozích zpráv:“ lze určit metodu, podle které má Avast rozlišovat odchozí zprávy od příchozích. Správné nastavení této volby je důležité pro korektní činnost celého programu, proto mu doporučujeme věnovat zvýšenou pozornost.

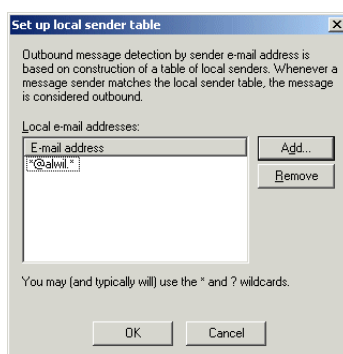
K dispozici jsou celkem tři možnosti:

- pomocí záhlaví zprávy („Received:“)
- pomocí odesílatelovy adresy
- pomocí IP adresy klienta (LAT)

Každá z těchto metod se liší způsobem, jakým se rozlišení provádí.

Volba „Pomocí záhlaví zprávy (“Received:”)“ určuje, že odchozí zpráv budou od odchozích rozlišovány pomocí (RFC 822) záhlaví zprávy, konkrétně záhlaví *Received*:. Bývá totiž zvykem, že každý SMTP server, přes který zpráva projde, do záhlaví zprávy vloží jednu položku *Received*:. Není-li tedy ve zprávě nalezena žádná takováto položka, zpráva pravděpodobně přes žádný SMTP server ještě neprošla, a jedná se tedy o odchozí zprávu.

Druhá metoda, kterou lze zapnout pomocí volby „Pomocí odesílatelovy adresy“ spočívá v rozlišení odchozí/příchozí zprávy podle e-mailové adresy jejího odesílatele. Je-li uživatel lokální, jde o odchozí zprávu; v opačném případě o zprávu příchozí. Aby tato metoda mohla fungovat, je pochopitelně nutné specifikovat lokální uživatele (tzn. sídlící na tomto serveru, případě v této organizaci). To se provádí pomocí tlačítka „Nastavit...“. Po jeho stisku se objeví okno „Nastavit tabulku lokálních odesílatelů“, v němž lze pomocí masek přesně nastavit, které e-mailové adresy jsou lokální (=interní) a které nikoliv. Např. pro server firmy ALWIL by bylo možno zapsat jednoduše masku **@alwil.**, která by postihla např. uživatele *user1@alwil.cz* a *user2@alwil.com*.

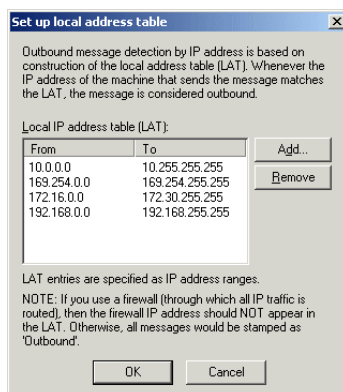


4.9 Okno „Nastavit tabulku lokálních odesílatelů“

Poslední nabízená metoda se aktivuje pomocí volby „Pomocí IP adresy klienta (LAT)“ a spočívá ve specifikaci interních IP adres Vaší sítě. Pokud se na server připojí někdo zevnitř sítě (tzn. někdo, jehož počítač je uveden v tabulce lokálních adres, zkráceně LAT z anglického Local Address Table), je jeho zpráva považována za odchozí. V opačném případě jde pravděpodobně o zprávu příchozí. Opět, aby mohla metoda úspěšně fungovat, je třeba správně nastavit její parametry pomocí tlačítka „Nastavit...“, v tomto případě konkrétně LAT. Je třeba upozornit, že používáte-li firewall nebo aplikační proxy (přes který se routuje veškerý IP provoz), potom by IP adresa firewallu *neměla* být součástí LAT. Jinak by jako odchozí byly označeny zprávy všechny, neboť všechny fakticky přicházejí z firewallu/proxy.

Další nastavení, které lze na stránce Upřesnit provést, se týká vkládání krátkých textových údajů na konec zpráv. Tyto zprávy mají vesměs informativní charakter a jejich použití závisí čistě na rozhodnutí správce sítě. Vkládání zpráv lze zapnout pro infikované příchozí zprávy, infikované odchozí zprávy, čisté příchozí zprávy a čisté odchozí zprávy.

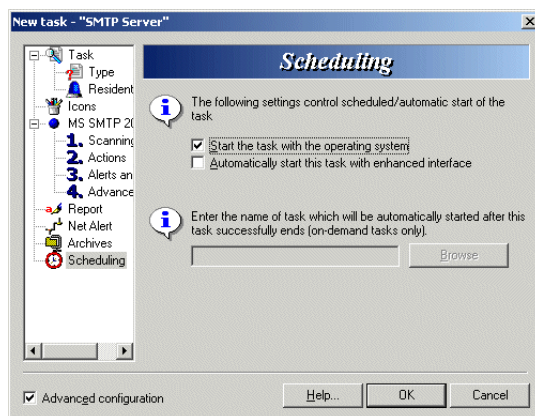
Poslední volba, „Přidávat informace do záhlaví zpráv“ určuje, zda má Avast přidávat do záhlaví každé otestované zprávy informace o výsledku testování. To může být užitečné např. pro automatický postprocessing.



4.10 Okno „Nastavit tabulku lokálních adres“

4.9 Stránka „Plánování“

Stránka „Plánování“ (obr. 4.11) obsahuje nastavení automatického spouštění a ukončování úloh.



4.11 Stránka „Plánování“

Zaškrtnutím pole „Spustit úlohu s operačním systémem“ uživatel sdělí programu, že vytvářená úloha má být spuštěna ihned po přihlášení uživatele. Implicitně není pole zaškrtnuto.

Zaškrťovací pole „Spustit úlohu při startu programu AVAST32“ zapíná spouštění úlohy automaticky po startu programu AVAST32. Spouštění úlohy zároveň s programem AVAST32 je implicitně vypnuto.

5 Použití Avastu pro MS SMTP Server

Tato kapitola podrobně popisuje praktické aspekty používání Avastu pro MS SMTP Server 2000.

5.1 Instalace při použití v režimu e-mail gateway

Účelem této kapitoly je objasnit, jak nakonfigurovat Vaši síť pro použití Avastu pro SMTP Server v režimu e-mail gateway. Tento režim je rozumné použít v jednom z následujících případů:

- Váš poštovní server Avast přímo nepodporuje. To může být buďto tím, že Vás poštovní server buďto není MS Exchange Server nebo Lotus Domino Server, nebo jím sice je, ale je provozován na jiné architektuře než Intel x86. V tom případě je použití Avastu jako e-mail gateway jednoduchá a ekonomická univerzální metoda, jak zamezit šíření poštovních virů ve Vaší organizaci.
- Provozujete sice Exchange nebo Lotus Domino server na Intelu, ale nechcete na něj (z jakéhokoli důvodu) nainstalovat Avast, např. proto, že se bojíte snížení výkonu, který už jen tak tak postačuje. I v tomto případě pro Vás Avast pro SMTP Server ve formě mail gateway představuje výhodné řešení ochrany.

Je potřeba hned zkraje říci, že pro provoz Avastu pro MS SMTP Server v režimu mail gateway budete pravděpodobně potřebovat dedikovaný počítač s instalovanými Windows 2000/XP Workstation nebo Server. Je pochopitelně možné poštu routovat i přes počítač, který nějaká osoba používá ke své práci, avšak toto nastavení příliš nedoporučujeme. Jednak proto, že uživatel by byl patrně negativně ovlivněn sníženým výkonem systému, způsobeným prací poštovního serveru a Avastu „na pozadí“, a jednak též proto, že klientské počítače bývají poměrně často restartovány (ať už proto, že dojde k „zamrznutí“ apod., nebo třeba proto, že uživatel instaluje nový software, který restart počítače vyžaduje). To je velmi nežádoucí, neboť nedostupnost poštovního serveru na tomto počítači (např. v době restartování) zablokuje veškerý poštovní provoz ve Vaší organizaci.

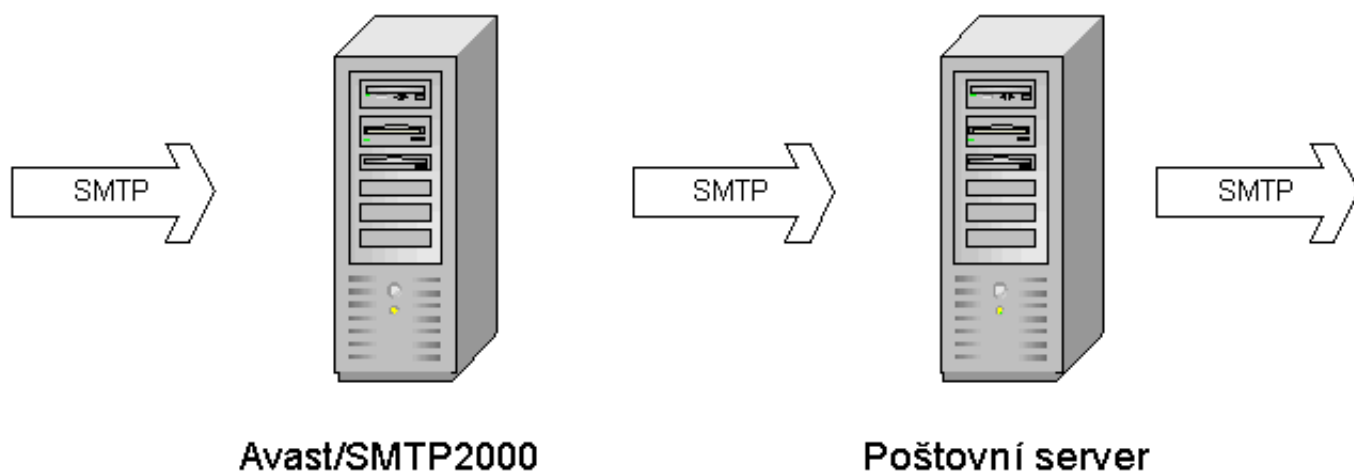
Shrneme-li uvedené požadavky, vidíme, že není nutno bezpodmínečně vyžadovat dedikovaný stroj, ale je nutno zajistit, že počítač bude vždy dostupný (highly-available) a bude mít vždy dostatek systémových prostředků (paměti, procesorového času), aby mohl úspěšně vyřídit všechny požadavky.

Vysvětleme nyní princip činnosti Avastu v režimu mail gateway. Jde o to, že všechna pošta ve Vaší organizaci (nebo alespoň její část, to závisí na Vaší volbě) bude routována přes počítač s instalovaným MS SMTP Serverem 2000 (standardní součást instalace Windows 2000/XP) a Avastem. MS SMTP Server 2000 bude samozřejmě nakonfigurován tak, že poštu nebude ukládat u sebe, ale všechny zprávy bude dále routovat, typicky na Vás skutečný SMTP server.

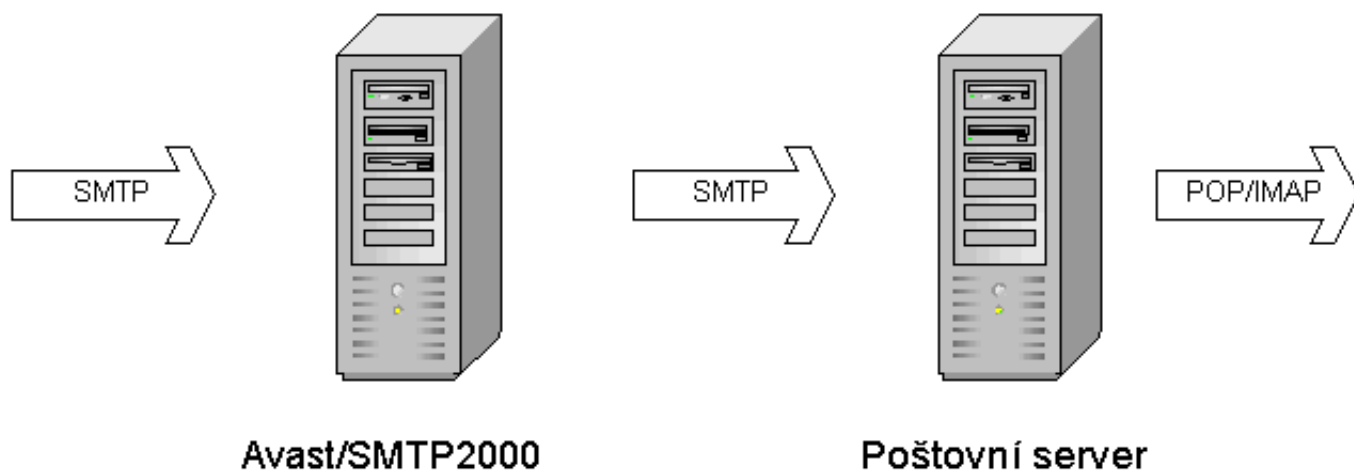
Možností, jak toho docílit, je několik a volba té konkrétní závisí jednak na Vás a jednak též na celkové topologii Vaší sítě. Nejtypičtější (a pravděpodobně v mnoha případech též nejjednodušší na nastavení) je model zobrazený na následujícím obrázku:

Zde tedy pošta zvenčí (příchodí) přichází nejprve na MS SMTP Server (Avast gateway), který ji po otestování dále posílá na hlavní poštovní server. Odchozí pošta je též nejprve

ávy



ávy



5.1

odesílána na MS SMTP Server (Avast e-mail gateway), který ji opět přeposílá na hlavní poštovní server, ze kterého potom odchází dál (nejčastěji do Internetu).

Při použití tohoto modelu je nutné zejména zajistit následující dvě věci:

- aby se pošta z Internetu posílala na MS SMTP Server místo na skutečný mail server, a
- aby klienti své zprávy odesílali místo na poštovní server na MS SMTP Server.

K tomu, jak tyto dvě věci zajistit, by Vám měly zpravidla stačit Vaše znalosti sítě, kteou spravujete. První bod lze zpravidla zajistit změnou MX recordu v DNS, případně je-li skutečný poštovní server v DMZ, změnou nastavení SMTP relayování na firewallu/aplikační proxy (SMTP). Situace je více méně stejná, jako kdybyste se rozhodli Váš opravdový

poštovní server přemístit z jednoho počítače (původního) na druhý (ten, na kterém je MS SMTP Server a Avast).

Co se týče druhého bodu, existuje opět několik metod, jak toho docílit. Nejpřímočarejší (ale nejpracnější) je „oběhnout“ všechny klienty a nastavení SMTP serveru v poštovních programech ručně změnit. To je však při větším množství počítačů velká práce, a tak je zpravidla vhodnější (je-li Váš mail server dedikovaný, tzn. neběží-li na něm žádný další serverový software, ke kterému by se klienti obraceli) změnit DNS jméno Vašeho mailserveru na něco jiného a původní jméno naopak přidělit počítači, na kterém je nyní MS SMTP Server a Avast. Tím začnou všichni klienti transparentně používat novou gateway (samozřejmě pouze za předpokladu, že odkaz na SMTP server není v klientských mailerech uveden ve formě IP adresy). Ve většině případů ale bohužel bývá SMTP server nastaven stejný jako POP3/IMAP server, a tento mechanismus tedy nebude správně fungovat, neboť MS SMTP Server s Avastem služby POP3/IMAP neposkytuje.

Druhou možností, jak message flow v organizaci uspořádat, je režim, kdy odchozí pošta bude nejprve routována na pravý server, který ji bude dál relayovat na MS SMTP Server 2000, a ten bude podle SMTP domény adresy dále rozhodovat, zda zprávu odeslat na internet (pomocí DNS) nebo, jde-li o lokálního příjemce, ji vrátit na původní server (MS SMTP Server obsahuje dostatečné prostředky k tomu, aby se takové věci daly nastavit).

Podstatné je, aby se pokud možno všechny zprávy routovaly přes SMTP Server s Avastem.

Postup instalace je tedy následující:

- Připravte stroj s Windows 2000/XP a nezapomeňte nainstalovat MS SMTP Service.
- Na tento počítač nainstalujte Avast, a to jak jádro, tak i plugin pro MS SMTP Server.
- Avast nakonfigurujte podle tohoto manuálu (kapitola Konfigurace rezidentní úlohy).
- Zvolte si způsob message flow a síť podle toho zkonfigurujte.
- Nezapomeňte zkonfigurovat MS SMTP Service. Např. pro první metodu routování (příchozí: Internet -> Avast -> mailserver, odchozí: klient -> Avast -> mailserver -> Internet) je potřeba na MS SMTP Serveru nastavit přeposílání na smart host a povolení anonymního relayování. Konkrétně v Control Panel -> Administrative Tools zvolte Internet Services Manager. Tam na „Default SMTP Virtual Server“ stiskněte pravé tlačítko a zvolte Properties. Na kartě Delivery zvolte Advanced a v kolonce Smart host vepište jméno Vašeho pravého poštovního serveru, na který bude tento service odesílat otestovanou poštu. Dále na kartě Access stiskněte tlačítko Relay a zvolte, aby právo relayovat měly všechny počítače (tzn. zvolte All except the list below a ujistěte se, že v seznamu nic není). Chcete-li použít druhou zmiňovanou metodu, musíte vytvořit pro SMTP server novou doménu (případně přejmenovat implicitní doménu) a nastavit smart host a relayování individuálně pro ní.

5.2 Instalace při použití v MS Exchange 2000

Při použití v MS Exchange 2000 Serveru je vše podstatně jednodušší, neboť Avast v tomto případě funguje jednoduše jako plugin do Exchange 2000. Pro jeho použití jej tedy stačí nainstalovat na počítač s funkčním Exchange 2000 Serverem a nakonfigurovat pro něj rezidentní úlohu (viz kapitola Konfigurace rezidentní úlohy). To je vše.

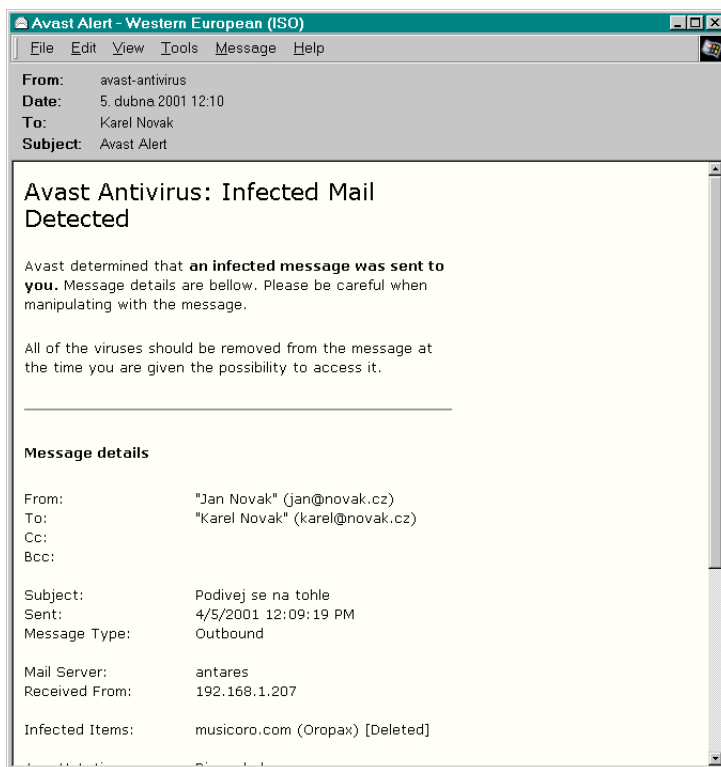
Jediná poznámka se týká koexistence s nativním pluginem Avastu pro MS Exchange 2000 Server (poskytovatelem „Exchange 2000“). Platí následující pravidla:

- Současnému používání poskytovatelů „Exchange 2000“ a „MS SMTP 2000“ v podstatě nic nebrání, snad pouze zbytečné dvojí skenování v případě SMTP zpráv.

- Poskytovatel „Exchange 2000“ vyžaduje na Exchange service pack 1 nebo vyšší. Není-li SP nainstalován, nemůžete tohoto poskytovatele použít.
- Poskytovatel „MS SMTP 2000“ chrání pouze SMTP provoz na serveru (tzn. výměnu poštovních zpráv, ale ne už např. zprávy z newsgroupů (NNTP), workflow objekty apod.). Naproti tomu poskytovatel „Exchange 2000“ by měl všechny tyto objekty chránit uniformně.
- Sami zjistíte, že poskytovatel „MS SMTP 2000“ má poněkud bohatší konfigurační možnosti, a je tedy podle našeho názoru pro ochranu SMTP provozu vhodnější.
- Poskytovatel „Exchange 2000“ nabízí také omezenou možnost skenování na serveru již uložených objektů (trochu ve smyslu „on-demand“ testování, i když v tomto případě o „on-demand“ ve skutečnosti nejde, protože se tyto testy vyvolávají automaticky po namountování IS. Jde prostě o jakési „skenování na pozadí“). Naproti tomu poskytovatel „MS SMTP 2000“ nic podobného nenabízí (a z podstaty věci ani nabízet nemůže, neboť se jedná o real-time filtr).
- Poskytovatel „Exchange 2000“ má tak chudé konfigurační možnosti, neboť je postaven na bázi rozhraní Microsoftu zvaného AVAPI (Antivirus Application Programming Interface) 2.0. Toto rozhraní bohužel neobsahuje všechny možnosti, které bychom si přáli. V současné době bohužel nezůstává než spokojit se s tím, co je (stejně jde o velký pokrok oproti AVAPI 1.0, obsaženého v Exchange 5.5 SP3 a lepší).

5.3 Používání notifikací

V případě, že Avast pro MS SMTP Server 2000 nalezne v nějaké zprávě virus (nebo zjistí, že zprávu nelze otestovat), a je-li to povoleno v nastavení konfigurace (viz konfigurační stránka „Akce“), odesílá Avast úhledné reporty o tom, že našel zavirovanou zprávu a že takové věci, jako šíření virů, se mezi slušnými lidmi prostě nedělají.



5.2 Implicitní notifikace, kterou Avast posílá odesílateli zavirované zprávy

Tyto notifikace obsahují dynamické informace, které jsou generovány v Avastem v závislosti na situaci. Standardně jsou reporty posílány v angličtině, protože ve většině případů Češi rozumí anglicky, ale bohužel ne naopak.

Notifikace lze však plně přizpůsobit Vaším představám (např. přeložit, rozšířit apod.). Chcete-li notifikační zprávy, které Avast posílá, změnit, stačí zeditovat soubory AvInf*.htm a AvUnt*, umístěné v adresáři <Avast32>\Data. Jde o zcela normální HTML soubory, takže pro jejich editaci lze použít libovolný nástroj k těmto účelům určený.

Konkrétně pro notifikace Avast pro SMTP 2000 Server používá následující soubory:

- *AvInfSnd.htm* - notifikace pro odesílate zavirované zprávy.
- *AvInfRec.htm* - notifikace pro příjemce zavirované zprávy.
- *AvInfOth.htm* - notifikace pro ostatní, v případě nalezení zavirované zprávy.
- *AvUntSnd.htm* - notifikace pro odesílate netestovatelné zprávy.
- *AvUntRec.htm* - notifikace pro příjemce netestovatelné zprávy.
- *AvUntOth.htm* - notifikace pro ostatní, v případě nalezení netestovatelné zprávy.

Dynamická data jsou v souborech samozřejmě nahrazována ad hoc až při odesílání notifikací Avastem. Pro jejich umístění se v notifikačních souborech používají tzv. šablony, neboli klíčová slova, která jsou za běhu programu dynamicky nahrazována skutečnými údaji. Pro soubory AvInf*.htm a AvUnt*.htm Avast rozeznává následující šablony:

- **%FROM%** - Adresa odesílatele zprávy (RFC822 záhlaví *From:*, příp. *Sender:*).
- **%TO%** - Adresa příjemce/příjemců zprávy (RFC822 záhlaví *To:*).
- **%CC%** - Obsah hodnoty záhlaví CC (carbon-copy).
- **%BCC%** - Obsah hodnoty záhlaví BCC (blind carbon-copy).
- **%SUBJECT%** - Předmět zprávy (RFC822 záhlaví *Subject:*).
- **%SENT%** - Datum a čas odeslání zprávy.
- **%TIMEDATE%** - datum a čas testování.
- **%TYPE%** - Informace, zda jde o příchozí (inbound) nebo odchozí (outbound) zprávu. Používá hodnoty deklarativních šablon **%INBOUND=%** a **%OUTBOUND=%**.
- **%SERVER%** - Jméno serveru, na kterém se provádí testování (z pohledu Avastu jméno lokálního počítače - vhodné v případě nasazení Avastu na více serverů).
- **%HOST%** - Adresa vzdáleného počítače, ze kterého SMTP požadavek na poslání zprávy vzešel (contacting host).
- **%ATTACH%** - Jméno (jména) infikovaného/netestovatelného objektu, včetně případného názvu viru, uvedeného v hranatých závorkách za jménem.
- **%ACTION%** - Akce, kterou Avast se zprávou provedl..
- **%VPS%** - datum a verze VPS souboru (virové databáze), který byl použit pro testování.

Kromě těchto jednoduchých šablon, jejichž výskyt v souboru je prostě nahrazen skutečnými daty, jsou ještě podporovány tzv. *deklarativní šablony*, které předdefinovávají určité hodnoty a jejichž výskyt je z konečné notifikace vždy odstraněn. Z tohoto důvodu mohou být v souboru umístěny na libovolném místě, třeba i za značkou </HTML>, určující konec HTML textu. Avast pro MS SMTP 2000 Server rozeznává následující deklarativní šablony:

- **%DELETED=Hodnota%** - hodnota určuje textový řetězec, který bude uveden u jména objektu při rozvíjení šablony **%ATTACH%** v případě, že virus nemohl nemohl být z objektu vyčištěn.
- **%CLEANED=Hodnota%** - hodnota určuje textový řetězec, který bude uveden u jména objektu při rozvíjení šablony **%ATTACH%** v případě, že virus byl z objektu úspěšně vyčištěn a infikovaná verze objektu byla ve zprávě nahrazena vyčištěnou.
- **%INBOUND=Hodnota%** - hodnota určuje textový řetězec, jímž bude nahrazena šablona **%TYPE%** v případě, že se jedná o příchozí zprávu.

- **%OUTBOUND=Hodnota%** - hodnota určuje textový řetězec, jímž bude nahrazena šablona **%TYPE%** v případě, že se jedná o odchozí zprávu.

Pro příklad použití těchto šablon můžete nahlédnout do implicitních souborů **AvInf*.htm** a **AvUnt*.htm**, které na disku vytváří instalační program a které používají všechny výše uvedené šablony.

5.4 Používání krátkých textů na konec zpráv

V současné době je poměrně populární trend, aby antivirový software vkládal na konec poštovních zpráv krátkou textovou informaci, jejímž úkolem je především ujistit příjemce, že zpráva neobsahuje virus. S touto myšlenkou poprvé přišla (alespoň pokud je nám známo) jedna nejmenovaná česká antivirová firma, a u zákazníků (ne všech) se setkala s poměrně pozitivním ohlasem. Avast pro SMTP Server 2000 tuto možnost též nabízí, a dovádí ji ještě dále: zprávičky lze totiž měnit podle libosti, a též podporují i formátované zprávy (HTML).

Můžete například zvolit, že všechny zprávy, které opustí brány Vaší organizace, budou opatřeny Vámi vytvořenou (nebo implicitní) zprávičkou, oznamující příjemci virovou čistotu zprávy (samozřejmě, je-li zpráva opravdu čistá...).

Systém definice zpráv je analogický definicím notifikací, viz sekce Používání notifikací. Pro zprávy se používají následující soubory:

- **AvInfTag.htm** - text připojený na konec (původně) zavirovaných zpráv s tělem ve formátu HTML.
- **AvInfTag.txt** - text připojený na konec (původně) zavirovaných zpráv s tělem ve formátu plain-text.
- **AvClnTag.htm** - text připojený na konec čistých (nezavirovaných) zpráv s tělem ve formátu HTML.
- **AvClnTag.txt** - text připojený na konec čistých (nezavirovaných) zpráv s tělem ve formátu plain-text.

Existují tedy samostatné verze zpráv pro body ve formátu HTML a plain-text (ve skutečnosti každá zpráva ve formátu HTML nese i ekvivalent v plain-textu, takže je-li formát body HTML, jsou Avastem připojeny obě verze, HTML i plain-text).

V těchto textech, podobně jako v případě notifikací, můžete používat šablony. V tomto případě je však množina přípustných šablon podstatně chudší, konkrétně jsou podporovány následující jednoduché šablony (jednoduše nahrazované Avastem skutečnými údaji):

- **%TIMEDATE%** - datum a čas testování.
- **%TYPE%** - Informace, zda jde o příchozí (inbound) nebo odchozí (outbound) zprávu. Používá hodnoty deklarativních šablon **%INBOUND=%** a **%OUTBOUND=%**.
- **%SERVER%** - Jméno serveru, na kterém se provádí testování (z pohledu Avastu jméno lokálního počítače - vhodné v případě nasazení Avastu na více serverů).
- **%VPS%** - datum a verze VPS souboru (virové databáze), který byl použit pro testování.

Kromě těchto jednoduchých šablon, jejichž výskyt v souboru je prostě nahrazen skutečnými daty, jsou ještě podporovány tzv. *deklarativní šablony*, které předdefinovávají určité hodnoty a jejichž výskyt je z konečného textu, připojovaného na konec zprávy, vždy odstraněn. Z tohoto důvodu mohou být v souboru umístěny na libovolném místě, v případě HTML verzí třeba i za značkou **</HTML>**, určující konec HTML textu. Pro případ zpráv se rozeznávají pouze dvě deklarativní šablony, související s jednoduchou šablonou **%TYPE%**:

- `%INBOUND=Hodnota%` - hodnota určuje textový řetězec, jímž bude nahrazena šablona `%TYPE%` v případě, že se jedná o příchozí zprávu.
- `%OUTBOUND=Hodnota%` - hodnota určuje textový řetězec, jímž bude nahrazena šablona `%TYPE%` v případě, že se jedná o odchozí zprávu.

5.5 Další vhodná nastavení Avastu

Pro efektivní použití Avastu pro SMTP server se doporučuje provést některá další nastavení. Typicky je vhodné zapnout prohlížení pakovaných souborů (např. ZIP). Mnoho souboru je v dnešní době komprimováno a aby mohl Avast tyto archívy procházet, musí to mít zapnuto (což implicitně pro většinu archívů *není*).

Občas může být užitečné zapnout generování tzv. zprávy, tzn. souboru, do kterého se podrobně zapisují jména všech objektů, které Avast během své činnosti otestoval, a též výsledek testování (zavirován x nezavirován, a v případě infekce i jméno viru).

Obě tyto volby, tzn. testování pakovaných souborů a generování zprávy se zapíná editací rezidentní úlohy, obsahující poskytovatele MS SMTP 2000 (naprosto stejně, jako u kterékoli jiné úlohy Avastu). Podrobný popis lze nalézt v manuálu k programu Avast32.

Rovněž je velmi podstatné zajistit pravidelnou aktualizaci virové databáze. V Avastu existuje několik způsobů aktualizace, můžete použít např. systém inkrementální aktualizace *iAVS*, který typicky virovou databázi stahuje přímo z Internetu (pro pravidelné spouštění použijte příkaz „Naplánovaná *iAVS*“ ve vlastnostech počítače v rozšířeném ovládní Avastu), nebo systém podnikové aktualizace pomocí souborů *.VPU*. Podrobný popis lze opět nalézt v manuálu ke standardnímu Avastu.