ESET MAIL SECURITY

PRO MICROSOFT EXCHANGE SERVER

Instalační manuál a užívatelská příručka

Microsoft® Windows® Server 2000 / 2003 / 2008 / 2008 R2

Pro stáhnutí nejnovější verze dokumentu klikněte zde

ESET MAIL SECURITY

ESET Mail Security byl vyvinut firmou ESET, spol. s r.o.

Pro více informací navštivte www.eset.cz.

REV. 1/8/2012

Obsah

1. Úvod

ESET Mail Security 4 pro Microsoft Exchange Server je integrovaným řešením, které chrání poštovní schránky uživatelů před různými typy škodlivého obsahu (nejčastěji jde o přílohy e-mailových zpráv infikované červy nebo trojany, dokumenty obsahující škodlivé skripty, phishing, spam, atd.). ESET Mail Security poskytuje tři typy ochrany: Antivirus, Antispam a aplikaci uživatelských pravidel. ESET Mail Security filtruje škodlivý obsah na úrovni poštovního serveru, dříve než se dostane do schránek klientů - příjemců e-mailu.

ESET Mail Security podporuje verze Microsoft Exchange Server versions 5.5 a novější, stejně jako Microsoft Exchange Server v prostředí klastrů (cluster environment). V novějších verzích Microsoft Exchange Server (2007 a novější) jsou podporovány i specifické úlohy (mailbox, hub, edge). ESET Mail Security se dá také vzdáleně spravovat pomocí ESET Remote Administrator.

Co se funkcionality týče, ESET Mail Security obsahuje všechny nástroje potřebné pro zabezpečení ochrany serveru i klienta (rezidentní ochrana, ochrana přístupu na web, ochrana e-mailových klientů a antispam) a navíc poskytuje i ochranu pre Microsoft Exchange Server.

1.1 Co je nové ve verzi 4.3 ?

ESET Mail Security ve verzi 4.3 obsahuje tyto novinky a vylepšení:

- Přepracované protokoly pro Antispam a Greylisting - nový typ protokolu obsahuje podrobnější informace o zprávě, která byla zaznamenaná do protokolu, včetně informací o důvodech, proč byla zpráva vyhodnocená jako spam.

- Automatické výjimky - přispívají k lepší stabilitě a hladšímu chodu serveru. Jedním kliknutím umožňuje zadat celou sadu výjimek ze skenování antivirovou ochranou pro specifické soubory nainstalovaných serverových aplikací a operačního systému.

- Kategorizace zpráv na základě hodnoty spam skóre - umožňuje administrátorovi přesně definovat hodnoty spam skóre od kterého bude zpráva vyhodnocena jako spam.

- Spojení licencí - ESET Mail Security umožňuje použít více licencí a rozšířiť tak množství chráněných poštovních schránek.

1.2 Systémové požadavky

Podporované operační systémy:

- Microsoft Windows NT 4.0 SP6, SP6a
- Microsoft Windows 2000 Server
- Microsoft Windows Server 2003 (x86 and x64)
- Microsoft Windows Server 2008 (x86 and x64)
- Microsoft Windows Server 2008 R2
- Microsoft Windows Small Business Server 2003 (x86)
- Microsoft Windows Small Business Server 2003 R2 (x86)
- Microsoft Windows Small Business Server 2008 (x64)
- Microsoft Windows Small Business Server 2011 (x64)

Podporované verze Microsoft Exchange Server:

- Microsoft Exchange Server 5.5 SP3, SP4
- Microsoft Exchange Server 2000 SP1, SP2, SP3
- Microsoft Exchange Server 2003 SP1, SP2
- Microsoft Exchange Server 2007 SP1, SP2, SP3
- Microsoft Exchange Server 2010 SP1, SP2

Nároky na hardware závisí na použité verzi Microsoft Exchange Server a také na nainstalovaném operačním

systému. Doporučujeme přečíst si dokumentaci k produktu Microsoft Exchange Server v případě, že potřebujete detailní informace o nárocích na hardware.

1.3 Metody ochrany

Pro kontrolu emailů se používají dvě nezávislé metody:

Kontrola poštovních schránok pomocí VSAPI 6
Filtrování zpráv na úrovni SMTP serveru 6

1.3.1 Kontrola poštovních schránek přes VSAPI

Kontrola poštovních schránek se spouští a je kontrolována Microsoft Exchange Serverem. Pošta v Microsoft Exchange Server store databázi se kontroluje průběžně. V závislosti na verzi Microsoft Exchange Serveru (i verze rozhraní VSAPI) a také na uživatelském nastavení, může být kontrola spuštěná v kterékoli z těchto situací:

- Pokud uživatel přistupuje k e-mailu, např. přes poštovní program (pošta vždy projde antivirovou kontrolou s aktuální virovou databází).
- Na pozadí, pokud je momentální vytížení Microsoft Exchange Servera nízké.
- Proaktivní (závisí na vnitřním algoritmu Microsoft Exchange Servera).

Rozhraní VSAPI se v současnosti využívá na antivirovou kontrolu a ochranu použitím pravidel.

1.3.2 Filtrování zpráv na úrovni SMTP serveru

Filtrování na úrovni SMTP serveru zabezpečuje specializovaný plugin. V Microsoft Exchange Server 2000 a Microsoft Exchange Server 2003 je to plugin (*Event Sink*) registrovaný na SMTP serveru jako součást Internet Information Services (IIS). V případě verzí Micrososft Exchange Server 2007/2010 je plugin registrován jako transportní agent na Microsoft Exchange Server v roli *Edge* nebo *Hub*.

Filtrování SMTP na úrovni serveru transportním agentem poskytuje antivirovou, antispamovou ochranu a ochranu pomocí pravidel, které nastaví sám uživatel. Na rozdíl od VSAPI filtrování, filtrování SMTP na úrovni serveru probíhá předtím než se kontrolovaná pošta doručí do mailového úložiště Microsoft Exchange Server (store).

1.4 Typ ochrany

Používají se tři hlavní typy ochrany:

1.4.1 Antivirová ochrana

Antivirová ochrana je jednou ze základních funkcí ESET Mail Security. Chrání uživatele proti útokům tak, že kontroluje soubory, emaily a internetovou komunikaci. Pokud je nalezena hrozba se škodlivým kódem, antivirový modul ji odstraní tak, že ji nejprve zablokuje a potom léčí/ vymaže nebo přesune do karantény 77.

1.4.2 Antispamová ochrana

Antispamová ochrana integruje více technologií (RBL, DNSBL, Fingerprinting, Reputation checking, Content analysis, Bayesian filtering, Manual whitelisting/blacklisting, aplikace pravidel, atd.) pro maximální přesnost detekce. Výstupem z antispamového skenovacího jádra je percentuální vyjádření pravděpodobnosti, že daný mail je SPAM (0 až 100). Pro účely EMSX jsou hodnoty nad 90 včetně považovány za dostatečné pro klasifikování mailu jako SPAM.

Součástí antispamové ochrany je i technika Greylisting (standardně vypnuta). Vychází ze specifikace RFC 821, podle které je SMTP protokol považován za nespolehlivý, a proto v případě dočasného selhání při pokusu o doručení mailu by se ho měl každý mailový agent pokusit doručit opakovaně. Podstatná část spamu je naopak doručována jednorázově (speciálními nástroji) a na množství adres získaných často automaticky "slovníkovým" způsobem. Poštovní server používající techniku Greylisting proto pro každou zprávu vypočítá kontrolní sumu (hash) pro trojici odesílatelů, příjemce a IP adresu odesílajícího MTA. Pokud server ve své databázi ještě takovou kontrolní sumu nemá, zprávu odmítne přijmout a vrátí kód dočasné chyby (temporary failure, např. 451). Legitimní odesílající server se po jistém čase pokusí zprávu doručit opakovaně a kontrolní suma se pro danou trojici zapíše do databáze ověřených spojení, tím se zaručí, že přicházející maily s touto charakteristikou jsou už doručovány okamžitě.

1.4.3 Uplatňování uživatelských pravidel

Ochrana pomocí uživatelských pravidel je dostupná při skenování pomocí VSAPI i při skenování transportním agentem. Uživatel může zadávat pravidla, které se dají navzájem kombinovat. Více podmínek v rámci jednoho pravidla bude propojeno pomocí logického operátoru AND, což znamená, že pravidlo bude provedeno pouze pokud budou splněny všechny jeho podmínky. Zadáním několika samostatných pravidel se aplikuje logický operátor OR, což znamená, že se provede první pravidlo, jehož podmínky jsou splněny.

V procesu kontroly je první použitou technikou greylisting - pokud je povolena. Dále v pořadí následuje ochrana pomocí uživatelských pravidel, antivirová kontrola a nakonec antispamová kontrola.

1.5 Uživatelské rozhraní

ESET Mail Security má grafické uživatelské rozhraní (graphical user interface - GUI) navrženo tak, aby bylo co nejvíce intuitivní.Toto GUI poskytuje rychlý a snadný přístup k hlavním funkcím programu.

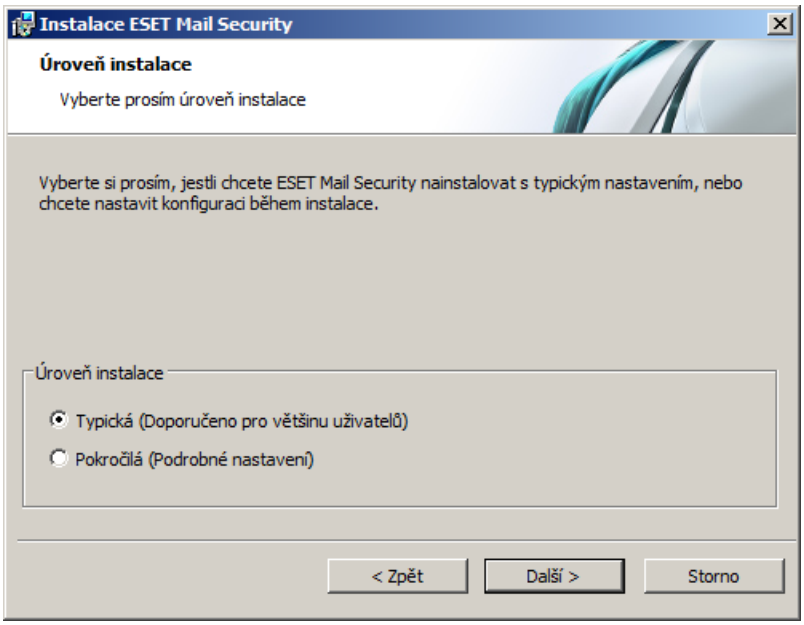
Kromě hlavního GUI je ještě k dispozici strom pokročilého nastavení, který lze otevřít kdykoli v programu stisknutím tlačítka **F5**.

Po stisknutí **F5** se objeví strom pokročilého nastavení, kde je možné vidět strukturu všech položek programu, které lze konfigurovat. Zde máte přístup ke všem volbám a možnostem, které můžete nastavit dle vašich potřeb. Z uspořádání položek je vidět, že struktura stromu je rozdělena na dvě hlavní větve, **Ochrana serveru** a **Ochrana počítače**. **Ochrana serveru** obsahuje položky, které se týkají nastavení ESET Mail Security specifických pro ochranu samotného Microsoft Exchange serveru. Větev **Ochrana počítače** obsahuje všechny nastavitelné položky pro "server jako počítač". To znamená, že se jedná o ochranu samotného serveru jako takového.

2. Instalace

Po zakoupení ESET Mail Security lze stáhnout instalační soubor ve formě .msi přímo ze stránky www.eset.cz. Po jeho spuštění se Vám zobrazí průvodce, který vás provede instalací a základními nastavením. Na výběr jsou 2 typy instalace s různými úrovněmi podrobnosti nastavení:

1. **Typická instalace**
2. **Volitelná instalace**



POZNÁMKA: Doporučujeme instalovat ESET Mail Security na nově instalovaný a nakonfigurovaný operační systém. V případě, kdy se ESET Mail Security instaluje na již existující systém, doporučujeme nejprve odinstalovat původní verzi ESET Mail Security, restartovat server a následně nainstalovat ESET Mail Security 4.5.

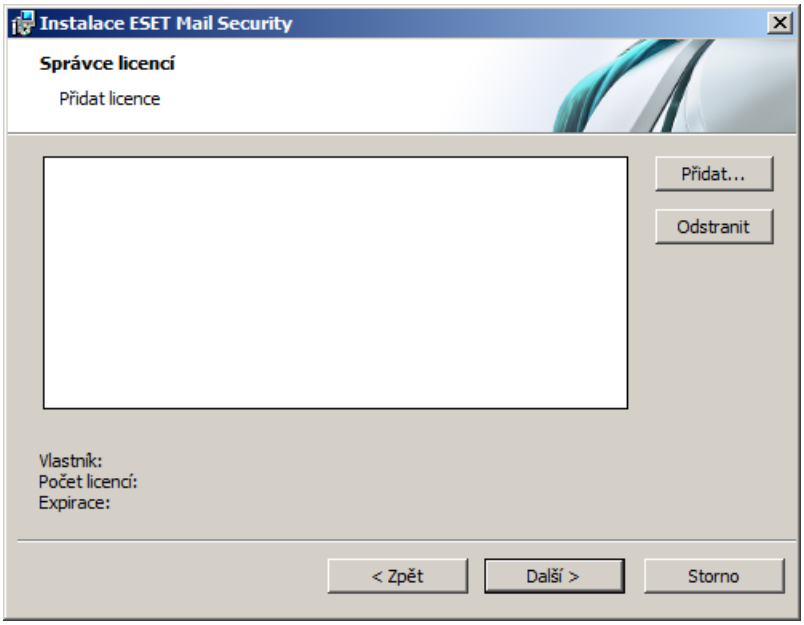
2.1 Typická instalace

Typická instalace je doporučena pro uživatele, kteří chtějí ESET Mail Security nainstalovat s typickým nastavením. Typické nastavení programu poskytuje maximální stupeň ochrany, což ocení zejména méně zkušení uživatelé, kteří nemají potřebu procházet podrobné nastavení.

Prvním, velice důležitým krokem instalace je **nastavení přihlašovacího jména** a **hesla** pro automatickou aktualizaci programu 65. Ta je podstatná pro zabezpečení stálé ochrany počítače.

Do položek **Uživatelské jméno** a **Heslo** je potřeba vyplnit přihlašovací údaje, které jste získali při zakoupení nebo registraci produktu. Pokud momentálně tyto údaje neznáte, označte políčko **Parametry aktualizace nastavit později**. Přihlašovací údaje můžete nastavit kdykoliv přímo z programu.

V dalším kroku instalace - **Licenční Manager** - přidejte licenci (*.lic soubor), který jste obdrželi na email po zakoupení produktu.



Dalším krokem instalace je nastavení systému včasného varování **ThreatSense.Net**, který umožňuje, aby společnost ESET, spol. s r. o. byla pohotově a neustále informována o nových infiltracích, a tak efektivněji chránila své zákazníky. Systém dovoluje odesílat nové druhy hrozeb do virové laboratoře společnosti ESET, spol. s r. o., kde se tyto hrozby analyzují a zapracovávají do virových databází

Označením políčka **Zapnout systém včasného varování ThreatSense.Net** systém aktivujete. V podrobných nastaveních máte možnost ovlivnit detaily posílání podezřelých souborů.

Třetím instalačním krokem je **nastavení možnosti detekce potenciálně nechtěných aplikací**. Potenciálně nechtěné aplikace představují programy, které ne vždy přímo představují bezpečnostní riziko, mohou však mít vliv na korektní fungování operačního systému. Obvykle jsou tyto aplikace instalovány po souhlasu uživatele během instalace jiného softwaru. Typicky může jít různé toolbary do prohlížeče a podobně.

Označením volby **Zapnout detekci potenciálně nechtěných aplikací** povolíte, aby ESET Mail Security detekoval i tento typ hrozeb.

POZNÁMKA: Pro zachování maximální bezpečnosti je doporučeno povolit detekci potenciálně nechtěných aplikací.

Posledním krokem typické instalace je potvrzení instalace programu tlačítkem **Instalovat**.

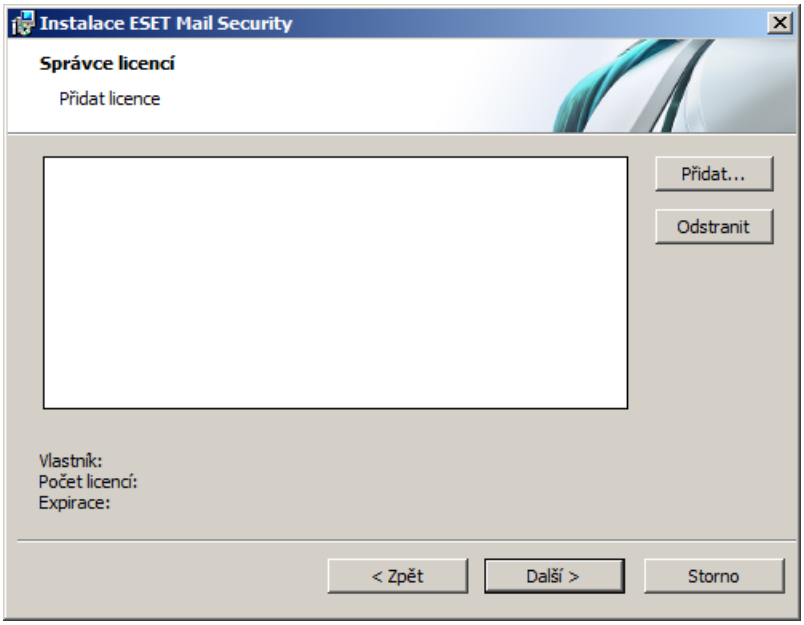
2.2 Pokročilá instalace

Je určená pouze pro zkušené uživatele, nesprávným nastavením, lze ohrozit bezpečnost počítače. Prvním krokem je nastavení umístění programu

Prvním krokem je nastavení umístění programu. Standardně se program instaluje do adresáře *C:\Program Files\ESET\ESET Mail Security*. Umístění je možné změnit prostřednictvím tlačítka **Prohledávat...**

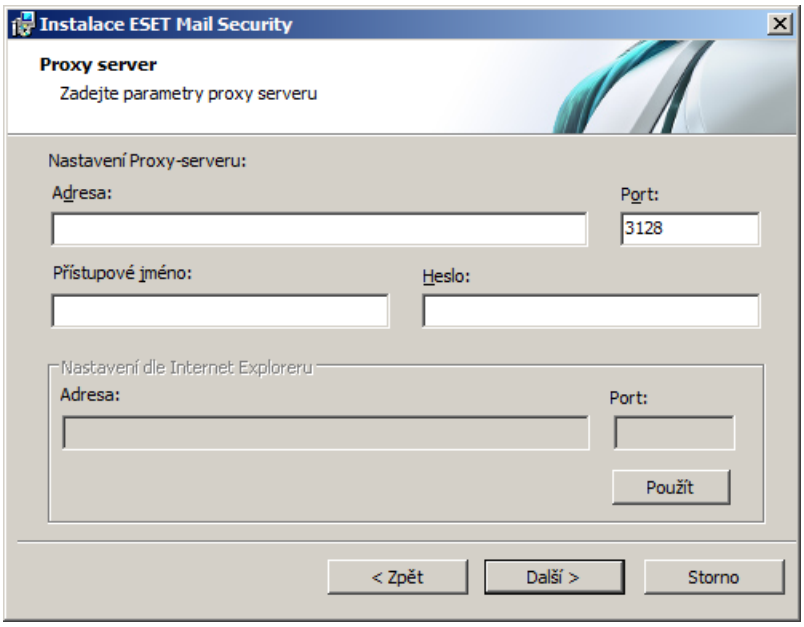
Následujícím krokem je **nastavení přihlašovacího jména a hesla**. Tento krok je shodný s Typickou instalací 8.

V dalším kroku instalace - **Licenční Manager** - přidejte licenci (*.lic soubor), který jste obdrželi na email po zakoupení produktu



Následuje **nastavení způsobu připojení do internetu**. Pokud používáte k připojení na internet telefoní linku, označte možnost **Na internet se připojuji pomocí telefoní linky**. V opačném případě ponechte možnost neoznačenou. Po zadání uživatelského jména a hesla, pokračujte konfigurací internetového připojení.

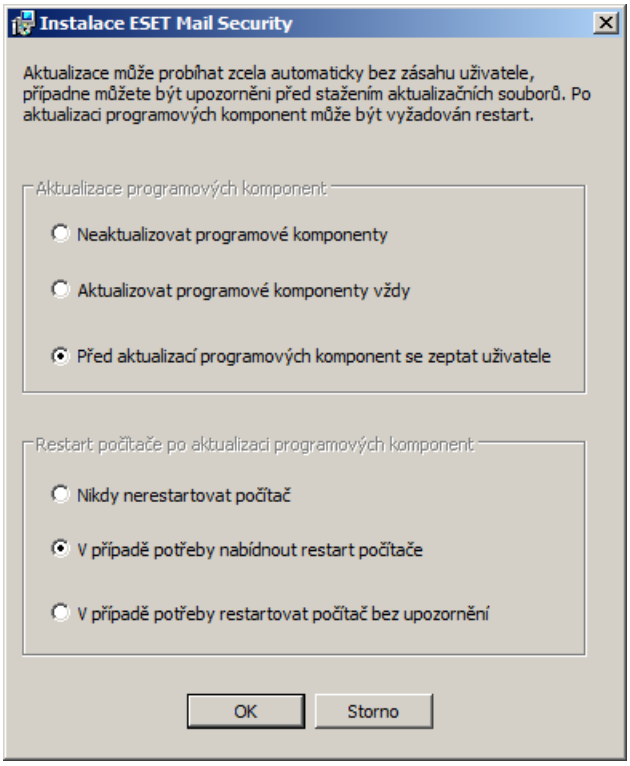
Nastavení proxy serveru je důležité pro správnou funkci aktualizace programu. V případě, že nevíte, zda pro připojení na internet používáte proxy-server, označte možnost **Nevím, zda používám proxy-server**, nastavení se převezme z nastavení Internet Exploreru. Pokud proxy server nepoužíváte, označte příslušnou možnost.



Pokud pro připojení proxy-serveru používáte a vybrali jste tuto možnost, v dalším kroku Vás instalátor požádá o upřesnění nastavení proxy-serveru. Do políčka **Addresa** vepište IP adresu nebo URL proxy serveru. Pole **Port** slouží k určení portu, na kterém proxy-server přijímá spojení (standardně 3128). Pokud proxy-server vyžaduje autentifikaci, je potřeba vyplnit pole **Uživatelské jméno** a **Heslo**. Proxy-server můžete nastavit i podle nastavení Internet Exploreru. Pokud si takto přejete nastavit proxy-server, klikněte na tlačítko **Použít** a potvrďte okno s výzvou.

Následujícím krokem instalace je nastavení automatické aktualizace programových komponentESET Mail Security nebo jinými slovy, automatický upgrade programu na novější verzi. Pomocí tlačítka **Změnit** otevřete podrobnější nastavení.

Pokud si nepřejete, aby se aktualizace programových komponent neprováděla automaticky, zvolte **Neaktualizovat programové komponenty**. Volbou **Upozornit před aktualizací programových komponent** si vyžádáte potvrzení stažení a instalace programových komponent. Automatickou aktualizaci programových komponent zajistíte volbou **Aktualizaci programových provést vždy**, když je k dispozici.



POZNÁMKA: Po aktualizaci programových komponent je obvykle vyžadován restart počítače. Doporučujeme zvolit možnost **Nikdy nerestartovat počítač**. Aktualizace programových komponent bude provedena po restartu počítače (manuálním nebo naplánovaném v Plánovači 75). Případně můžete zvolit **V případě potřeby nabídnout restart počítače** pokud si přejete být informováni o potřebě restartu po aktualizaci programových komponent. Při tomto nastavení máte možnost restartovat server podle potřeby buď ihned, nebo odložit restart a vykonat jej později.

Dalším krokem instalace je **nastavení hesla pro ochranu nastavení** programu. Zvolte heslo, které bude vyžadováno při každém změně nebo přístupu do nastavení ESET Mail Security.

Kroky instalace pro **Nastavení ThreatSense.Net** a **Detekci potenciálně něchtěných aplikací** jsou shodné s Typickou instalací 8.

Následuje poslední krok instalace, vyžadující potvrzení pro instalaci programu.

2.3 Terminálový server

Pokud používáte ESET Mail Security na Windows serveru, který slouží i jako Terminálový server, můžete využít možnost deaktivace grafického rozhraní ESET Mail Security, čímž zabráníte jeho opakovanému spouštění při každém přihlášení uživatele. Návod jak deaktivovat grafické rozhraní naleznete v kapitole Terminálový server v části Deaktivace grafického rozhraní 102.

2.4 Aktualizace na novější verzi

Novější verze ESET Mail Security jsou vydávány za účelem zdokonalení produktu a opravy chyb, které nelze opravit v rámci automatické aktualizace programových modulů. Je několik způsobů, jak aktualizovat produkt na novější verzi:

1. Automaticky prostřednictvím aktualizace programových komponent (PCU)
   Aktualizace programových komponent se týká všech uživatelů daného produktu a může mít významný dopad na systém. Je vydávána až po dlouhém období testování na všech operačních systémech v různých konfiguracích. Pokud potřebujete aktualizovat na nejnovější hned po jejím vydání, použijte některou z následujících metod.

2. Manuálně stáhnutím a přeinstalací stávající verze novou z www.eset.cz .
   Na začátku přeinstalace je možné zvolit zachování aktuálních nastavení programu (volba **Použít původní nastavení**).

3. Manuálně s automatickou vzdálenou instalací na stanice v síti prostřednictvím ESET Remote Administrator.

2.5 Instalace v prostředí clusterů

Cluster je skupina serverů (serveru zapojenému v clusteru se říká "node" - "uzel"), které fungují společně jako jeden server. Takové prostředí poskytuje vysokou dostupnost a spolehlivost poskytovaných služeb. Pokud jeden z uzlů v clusteru selže nebo se stane nedostupný, jeho funkci automaticky převezme další. ESET Mail Security plně podporuje MS Exchange Servery zapojeny do clusteru. Důležité je, aby měl ESET Mail Security na všech uzlech v clusteru stále stejnou konfiguraci. To je možné zajistit prostřednictvím ESET Remote Administrator (použitím policy). V následujících částech si ukážeme, jak nainstalovat a nakonfigurovat ESET Mail Security na uzly v clustery pomocí ESET Remote Administrator (ERA).

Instalace

V této kapitole je popsána Push instalace, není to však jediný způsob jak nainstalovat produkt na cílový počítač. Podrobnější informace naleznete v dokumentaci k ESET Remote Administrator.

1) Na počítač s ERA stáhněte msi instalační balíček ESET Mail Security z webové stránky ESETu. V ERA v záložce **Remote Install** v části **Computers** klepněte pravým tlačítkem na libovolné místo do seznamu počítačů av kontextovém menu vyberte možnost **Manage Packages**. V menu **Type** zvolte **ESET Security Products package**, klepněte na **Add ...** a jako **Source** vyberte stažený msi instalační balíček ESET Mail Security. Klikněte na **Create**.

2) V části **Edit / Select configuration Associated with this package** zvolte Edit a nakonfigurujte nastavení **ESET Mail Security** dle Vašich potřeb. V konfiguračním editoru se nastavení týkající se ESET Mail Security nacházejí ve větvi **ESET Smart Security, ESET NOD32 Antivirus> Mail server protection a Mail server protection for Microsoft Exchange Server**. Samozřejmě je možné nastavit i parametry dalších modulů, které ESET Mail Security obsahuje (např. Update module, Computer scan atd..). Nakonfigurováno nastavení doporučujeme vyexportovat do xml souboru, který je později možné použít např. při vytváření instalačního balíku (Installation Package), aplikování konfigurační úlohy (Configuration Task) nebo politiky (Policy).

3) Klikněte na **Close**, v dialogovém okně s otázkou **Do you want to save the package into server?** zvolte **Yes** av následujícím okně vyberte název instalačního balíčku. Instalační balíček se pod zvoleným názvem a se zadefinovanou konfigurací uloží na server a je připraven k použití. Nejčastějším je použití přímo při vzdálené instalaci (Push Install), ale lze jej také samostatně uložit jako klasický msi instalační balíček a použít při přímé instalaci na serveru (volba **Save As ...** v **Installation Packages Editor> Create / Select installation package content**) .

4) Keď máme takto pripravený inštalačný balík, môžeme spustiť jeho vzdialenú inštaláciu na uzly v clusteri. V ERA v časti **Remote Install**, záložka **Computers** označíme uzly na ktoré chceme ESET Mail Security vzdialene nainštalovať (Ctrl + klik ľavým tlačítkom myši). Kliknite pravým tlačítkom na ľubovoľné miesto do zoznamu počítačov a v kontextovom menu vyberte možnosť **Push Installation**. Pomocou **Set** / **Set All** nastavíme používateľské meno a heslo užívateľa na cieľovej stanici – uzle, pod ktorým prebehne push inštalácia (musí to byť používateľ s administrátorskými právami). V ďalšom kroku zvolíme inštalačný balíček a v nasledujúcom kroku spustíme vzdialenú inštaláciu. Inštalačný balíček obsahujúci ESET Mail Security s nadefinovanou konfiguráciou bude nainštalovaný na zvolené cieľové stanice - uzly. Po krátkom čase sa ESET Mail Security z cieľových staníc objavia medzi klientami v ERA (záložka **Clients**) a je možné ich vzdialene menežovať.

4) Když máme takto připravený instalační balíček, můžeme spustit jeho vzdálenou instalaci na uzly v clusteru. V ERA v části **Remote Install**, záložka **Computers** označíme uzly na které chceme ESET Mail Security vzdáleně nainstalovat (Ctrl + klik levým tlačítkem myši). Klikněte pravým tlačítkem na libovolné místo do seznamu počítačů a v kontextovém menu vyberte možnost **Push Installation**. Pomocí **Set / Set All** nastavíme uživatelské jméno a heslo uživatele na cílové stanici - uzlu, pod kterým proběhne push instalace (musí to být uživatel s administrátorskými právy). V dalším kroku zvolíme instalační balíček a spustíme vzdálenou instalaci. Instalační balíček obsahující ESET Mail Security s nadefinovanou konfigurací bude nainstalován na zvolené cílové stanice - uzly. Po krátkém čase se ESET Mail Security z cílových stanic objeví mezi klienty v ERA (záložka **Clients**) a je možné je vzdáleně spravovat.

POZNÁMKA: Pro bezproblémový průběh vzdálené instalace je třeba splnit několik podmínek jako na straně cílové stanice, tak i na straně ERA Serveru. Podrobnější informace naleznete v dokumentaci k ESET Remote Administrator.

Konfigurace

Pro správné fungování ESET Mail Security na uzlech v clusteru je důležité, aby byly stále stejně nakonfigurovány. Pokud jste dodrželi výše uvedený postup, je tato podmínka splněna. Stále však hrozí, že na jednom z uzlů bude tato konfigurace omylem pozměněna a dojde tak k inkonzistenci nastavení mezi jednotlivými ESET Mail Security v clusteru. Tomuto se dá vyhnout použitím policy v ESET Remote Administrator. Policy se v mnohém podobá běžnou konfigurační roli (Configuration Task) - jde o vyslání konfigurace definované v konfiguračním editoru (Configuration Editor) na klienta / klienty. V případě policy se však nejedná o jednorázové vyslání konfigurace, ale o celkové zabezpečení určité konfigurace spravovaných ESET security produktů. Policy bychom tedy mohli definovat jako konfiguraci, která je neustále vnucována klientovi / skupině klientů.

V **Tools> Policy Manager...** existuje několik možností jak použít policy. Nejjednodušší možností je využít **Default Parent Policy**, která standardně slouží i jako **Default policy for Primary Clients**. Tato policy má tu vlastnost, že se automaticky aplikuje na všechny přímo připojené klienty - tj. v našem případě na vzdáleně nainstalované ESET Mail Security na uzlech v clusteru. Policy lze nakonfigurovat po stisku tlačítka **Edit ...**, přičemž lze využít již existující konfiguraci uloženou v xml souboru, pokud jsme si ji předtím vytvořili. Druhou možností je vytvořit si novou policy (**Add New Child Policy**) a pomocí **Add Clients ...** jí přiřadit všechny ESET Mail Security na serverech v clusteru.

Tato konfigurace zajistí, že na všech klientech bude prostřednictvím jedné policy aplikováno stejné nastavení. Pokud v budoucnu budeme chtít změnit nastavení v ESET Mail Security v clusteru, stačí změnit danou policy. Změny se přenesou na všechny klienty spadajících pod danou policy.

POZNÁMKA: Podrobnější informace k využití policies naleznete v dokumentaci k ESET Remote Administrator.

2.6 Licence

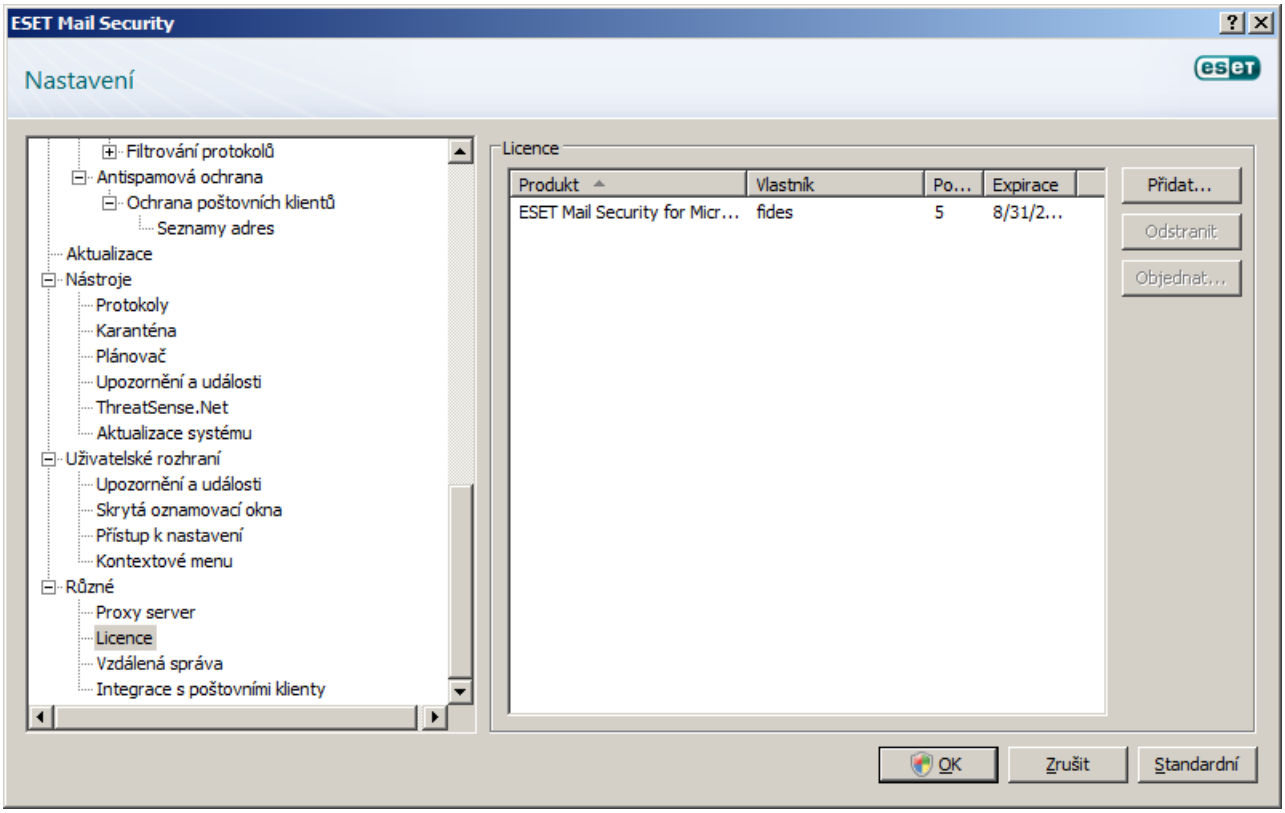
Velmi důležitý krok je vložení licenčního souboru pro ESET Mail Security for Microsoft Exchange Server. Bez licence nebude ochrana pošty na systému Microsoft Exchange Server fungovat správně. Pokud nevložíte licenci do produktu během instalace, můžete tak učinit později v rozšířených nastaveních v části **Různé> Licence**.

ESET Mail Security umožňuje použít více licencí najednou, přičemž ke spojení může dojít jedním z následujících způsobů:

1) Dvě nebo více licencí pro jednoho zákazníka (tj. se stejným zákaznickým jménem) se sčítají, tj. zvýší počet kontrolovaných mailboxů, a vyhodnotí se jako jedna. V licenčním manažeru však budou tyto licence stále figurovat samostatně.

2) Dvě nebo více licencí pro různé zákazníky. Spojují se stejným způsobem jako licence pro jednoho zákazníka s tím rozdílem, že ke spojení licencí dojde pouze pokud alespoň jedna ze spojovaných licencí obsahuje speciální atribut umožňující spojování licencí od různých zákazníků. O vygenerování licence s takovým atributem je třeba požádat Vašeho prodejce.

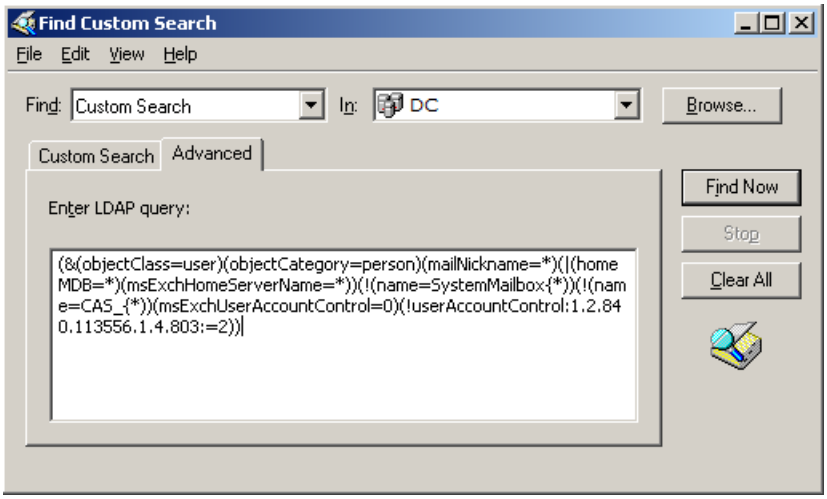
POZNÁMKA: Platnost spojených licencí se vypočítává podle licence s nejkratší platností.



ESET Mail Security porovnává počet poštovních schránek v active directory s počtem poštovních schránek definovaných v použité licenci. Pokud je v soustavě napojeno více Exchange serverů, při zjišťování celkového počtu poštovních schránek se bere v úvahu i počet poštovních schránek těchto Exchange serverů. Systémové poštovní schránky, deaktivovány poštovní schránky a emailové aliasy se do počtu použitých poštovních schránek nezapočítávají. V prostředí clusteru se uzly s rolí "clustered mailbox" do počtu použitých poštovních schránek nezapočítávají.

Počet použitých poštovních schránek v MS Exchange lze zjistit takto. Na serveru otevřete **Active Directory Users and Computers**. Pravým tlačítkem myši na doménu av kontextovém menu zvolte **Find ...**. V roletovém menu Find menu zvolte **Custom Search** a klikněte na záložku **Advanced**. Do textového pole nakopírujte následující LDAP (Lightweight Directory Access Protocol) požadavek a stiskněte **Find Now**:

- `(&(objectClass=user)(objectCategory=person)(mailNickname=*)(|(homeMDB=*)(msExchHomeServerName=*))(!(name=SystemMailbox{*))(!(name=CAS_{*))(msExchUserAccountControl=0)(!userAccountControl:1.2.840.113556.1.4.803:=2))`



Pokud počet poštovních schránek v active directory překročí počet poštovních schránek definovaných v licenci, do logu Microsoft Exchange Serveru se zapíše hlášení "Protection status changed due to exceeded number of Mailboxes (count) covered by your license (count).". Zároveň se v ESET Mail Security změní **Stav ochrany** na **ORANŽOVOU** a zobrazí se zpráva informující o 42 denní lhůtě, po jejímž uplynutí bude ochrana vypnuta. V takovém případě doporučujeme kontaktovat prodejce a rozšířit si licenci o chybějící počet poštovních schránek.

Pokud během 42 denní lhůty nebude vložena nová licence pokrývající chybějící poštovní schránky, **Stav ochrany** změní barvu na **ČERVENOU** a zobrazí se zpráva o vypnutí ochrany z důvodu překročení počtu poštovních schránek. V takovém případě doporučujeme okamžitě kontaktovat prodejce a zajistit rozšíření licence o chybějící počet poštovních schránek.

2.7 Nastavení po instalaci

Pro zajištění optimální funkčnosti a maximální ochrany je třeba po instalaci produktu vhodně nakonfigurovat některá základní nastavení.

Nastavení Antispamu

Tato část popisuje nastavení, metody a techniky, které můžete použít na ochranu Vaší sítě před spamem. Doporučujeme Vám, abyste si přečetli všechny následující instrukce dříve, než si vyberete tu nejvhodnější kombinaci nastavení pro Vaši síť.

Správa spamu
Pro optimální fungování antispamové ochrany je nutné definovat, jak budou dále zpracovány zprávy vyhodnoceny jako SPAM.

K dispozici jsou následující tři možnosti:

1. **Vymazávaní spamu**

   Vzhledem k tomu, že hranice na posouzení zprávy jako SPAM je v ESET Mail Security nastavena bezpečně vysoko, je riziko smazání legitimní zprávy minimální. Platí zde pravidlo, že čím podrobnější jsou specifikovány nastavení antispamu, tím je menší pravděpodobnost, že bude vymazána legitimní pošta. Mezi výhody této metody patří její nenáročnost na systémové prostředky a méně času stráveného administrací. Nevýhodou je, že pokud dojde k případnému smazání legitimní zprávy, není ji možné lokálně obnovit.

2. **Karanténa**

   Tato možnost vylučuje riziko vymazání legitimní pošty. Zprávy se dají okamžitě obnovit a přeposlat původnímu příjemci. Nevýhodami této metody jsou vyšší zatížení Microsoft Exchange Serveru a dodatečný čas potřebný k údržbě e-mailové karantény. Na přesunutí mailu do karantény můžete využít dva způsoby:

   A. Interní karanténa Microsoft Exchange Serveru (platí pouze pro Microsoft Exchange Server 2007/2010): - pokud chcete použít interní karanténu serveru ujistěte se, že pole **Společná karanténa zpráv** v pravé části okna menu rozšířených nastavení (**Ochrana serveru> Karanténa zpráv**) je prázdné a aktivujte volbu **Uložit do systémové karantény zpráv poštovního serveru** z rozbalovacího menu v dolní části. Tato metoda funguje pouze v případě, že interní karanténa Exchange serveru existuje. Exchange server standardně nemá tuto interní karanténu aktivovanou. Pokud ji chcete aktivovat, je potřeba otevřít Exchange Management Shell a zadat následující příkaz:

      Set-ContentFilterConfig -QuarantineMailbox nazev@domena.cz

      (nahraďte nazev@domena.cz skutečným názvem poštovní schránky, která bude použita Microsoft Exchange serverem jako interní karanténa, např. exchangekarantena@spolecnost.cz)

   B. Vlastní poštovní schránka karantény:
      - pokud zadáte adresu do pole **Společná karanténa zpráv**, ESET Mail Security začne přesouvat všechny nové zprávy do této zadefinované emailové schránky.

      Podrobnější informace o karanténě si lze přečíst v kapitole Karanténa zpráv 23.

3. **Přeposílání spamu**

   Spam se bude přeposílat dále do organizace s tím, že ESET Mail Security do každé zprávy doplní příslušný MIME header s SCL hodnotou, na jejímž základě pak IMF (Intelligent Message Filtering) Exchange Serveru provede příslušné akce.

Filtrování spamu

Antispamové jádro

Antispamové jádro nabízí tři konfigurace - **Doporučená, Maximální přesnost** a **Maximální rychlost**. V případě, že není nutné optimalizovat konfiguraci na maximální propustnost (např. při zvýšené zátěži serveru), doporučujeme vybrat konfiguraci **Maximální přesnost**. Při konfiguraci **Doporučená** si antispamové jádro dolaďuje konfiguraci automaticky na základě skenovaných zpráv. Pokud je zapnuta možnost **Maximální přesnost** nastavení se optimalizují s ohledem na co nejspolehlivější detekci. Extra výběr **Vlastní> Otevřít konfigurační soubor** umožní uživateli upravit soubor spamcatcher.conf 39. Tuto možnost doporučujeme pouze pro pokročilé uživatele.

Před spuštěním plného provozu serveru Vám doporučujeme nastavit seznamy blokovaných a povolených IP adres:

1) Otevřete okno rozšířených nastavení programu av něm sekci **Antispamová ochrana**. Označte pole **Chránit server pomocí antispamové ochrany**.
2) Klikněte na sekci **Antispamové jádro.**
3) Kliknite na tlačidlo **Nastaviť...** definujte **Povolené, Ignorované** a **Blokované IP adresy.**
   - Na záložce **Blokované IP adresy** můžete přidávat IP adresy, které by měly být blokovány, tj. jestliže jakákoli neignorovaná IP adresa v přijatých hlavičkách (Received headers) souhlasí s kteroukoliv adresou v tomto seznamu, zprávě se přidělí skóre 100 a již neprobíhají žádné další kontroly.
   - Na záložce **Povolené IP adresy** můžete přidávat IP adresy, které mají mít statut povoleno, tj. pokud první neignorovaná IP adresa v přijatých hlavičkách (Received headers) souhlasí s kteroukoliv adresou v tomto seznamu, zprávě se přidělí skóre 0 a více se již nekontroluje.
   - Na záložce **Ignorované IP adresy** můžete přidávat IP adresy, které budou ignorovány během RBL kontroly (Real-time Blackhole List (RBL) checks). V tomto seznamu by se měly nacházet všechny interní IP adresy firewallu, které nejsou přímo dostupné z Internetu. Přidáním takových adres zabráníte zbytečným kontrolám interních IP adres a umožníte systému identifikovat připojující se externí IP adresy.

Greylisting

Greylisting je metoda, která chrání uživatele před spamem pomocí následující techniky: Transportní agent posílá návratovou SMTP hodnotu Temporarily rejected ('dočasně zamítnuta' = přednastavená je hodnota 451/4.7.1) na každou přijatou zprávu, která nepochází z identifikovaného zdroje. Legitimní odesílající server se po jistém čase pokusí zprávu znovu doručit. Spamové servery se obvykle nepokoušejí tyto zprávy při neúspěšném doručení znovu odeslat, protože odesílají tisíce emailových adres najednou a nemají čas na zpětnou kontrolu.

Při vyhodnocování zdroje zprávy se berou v úvahu nastavení na seznamech: **Povolené IP adresy, Ignorované IP adresy**, seznamy **Safe Senders** a **Allow IP** definované na Exchange Serveru, a také nastavení AntispamBypass pro daný mailbox. Greylisting je metoda, která musí být pečlivě nastavena, jinak může mít za následek nežádoucí efekty jako je pozdržení doručení zpráv z legitimních zdrojů nebo od známých odesílatelů. Tento efekt bude postupem času ustupovat zároveň s tím, jak si bude metoda budovat interní whitelist ověřených spojení. V případě, že vám daná metoda není známa, nebo zmíněný vedlejší efekt pro vás není přípustný, doporučujeme metodu vypnout v menu rozšířených nastavení pod **Antispamová ochrana> Microsoft Exchange Server> Transportní agent> Povolit techniku Greylisting.**

Rovněž doporučujeme metodu vypnout, pokud produkt používáte jen na otestování funkcionality a nechcete nastavovat rozšířené funkcionality programu.

POZNÁMKA: Greylisting je jen doplňkovou vrstvou ochrany před spamem a nemá žádný vliv na hodnotící schopnosti antispamového modulu.

Nastavení antivirové ochrany

Karanténa

V závislosti na zvoleném režimu léčení doporučujeme definovat v nastaveních akci, která bude aplikována na infikované (neléčené) zprávy. Tuto možnost najdete v rozšířeném menu pod **Ochrana serveru> Antivirus a antispyware> Microsoft Exchange Server> Transportní agent.**

Pokud je možnost posílat zprávy do emailové karantény aktivní, je nezbytné definovat karanténu v menu rozšířených nastavení v sekci **Ochrana serveru> Karanténa zpráv.**

Výkon
Pokud tomu nebrání jiné omezení, doporučujeme vám zvýšit počet ThreatSense skenovacích jader v menu rozšířených nastavení (**F5**) pod **Ochrana serveru> Antivirus a antispyware> Microsoft Exchange Server> VSAPI> Výkon** podle následujícího vzorce: *počet vláken kontroly = (počet fyzických CPU x 2) + 1*. Počet vláken kontroly by měl být stejný jako počet ThreatSenseskenovacích jader. Počet skenovacích jader můžete nastavit pod **Ochrana počítače> Antivirus a antispyware> Výkon.**

Například:
Máte server se 4 fyzickými CPU. Nejlepšímu výkonu, po použití výše uvedeného vzorce, by odpovídalo 9 vláken kontroly a 9 skenovacích jader.

POZNÁMKA: Doporučujeme nastavení počtu skenovacích jader ThreatSense tak, aby byl shodný s počtem použitých vláken kontroly. Pokud použijete větší počet vláken kontroly než skenovacích jader, nebude to mít žádný pozitivní vliv na výkon

POZNÁMKA: V případě, že používáte ESET Mail Security na Windows serveru, který slouží jako Terminálový Server, a nechcete aby se startovalo ESET Mail Security GUI pokaždé jak se uživatel přihlásí, tak toto startování GUI můžete vypnout. Detailní postup jak vypnout GUI si přečtěte v kapitole Vypnutí GUI na terminálovém serveru 102.

3. ESET Mail Security - ochrana pro Microsoft Exchange Server

ESET Mail Security poskytuje vašemu serveru Microsoft Exchange široké spektrum ochrany. Mezi tři nejzákladnější typy ochrany patří Antivirus, Antispam a uživatelské pravidla. ESET Mail Security zajišťuje ochranu před nejrůznějšími typy škodlivého softwaru, včetně příloh e-mailů napadených červy nebo trojskými koňmi, dokumentů obsahujících škodlivé skripty, phishingu a spamu. ESET Mail Security filtruje škodlivý obsah na úrovni e-mailového serveru, dříve než se může dostat do schránky poštovního klienta příjemce. V dalších kapitolách popíšeme všechny dostupné možnosti a nastavení, díky kterým si budete moci přizpůsobit a doladit ochranu vašeho Microsoft Exchange serveru přesně podle vašich představ.

3.1 Všeobecná nastavení

Tato část blíže popisuje jak zacházet s pravidly, soubory s protokoly, karanténu zpráv a nastavení výkonu.

3.1.1 Microsoft Exchange Server

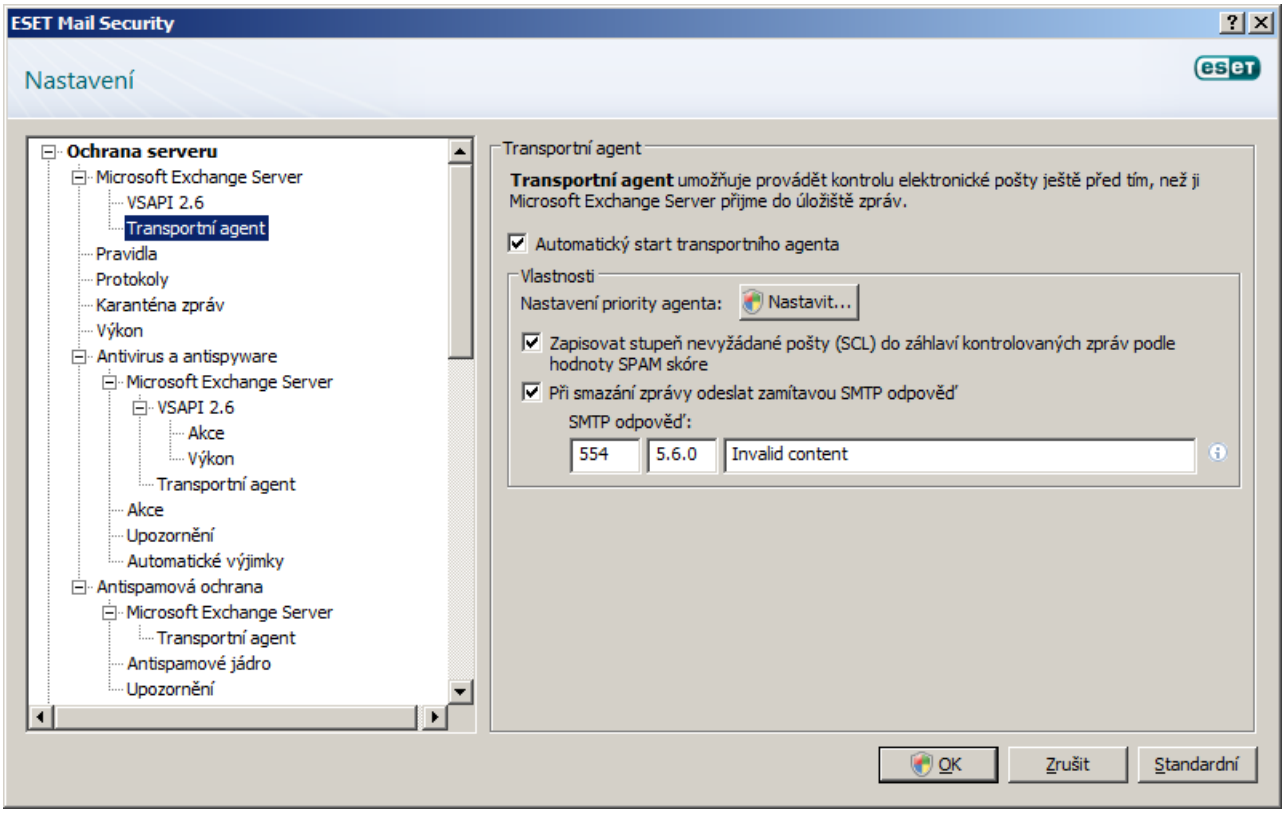
3.1.1.1 VSAPI (Virus-Scanning Application Programming Interface)

Microsoft Exchange Server je vybaven mechanismem, který zajišťuje, že každá část zprávy se překontroluje nejnovější virovou databází. Pokud zpráva nebo její část ještě nebyla zkontrolována, tato bude oskenování dříve než se uvolní pro klienta. Každá podporovaná verze Microsoft Exchange Server (5.5/2000/2003/2007/2010) nabízí odlišnou verzi VSAPI.

Pomocí zaškrtávacího pole v pravé části okna kontrolujete automatický start té verze VSAPI, kterou používá Váš Exchange server.

3.1.1.2 Transportní agent

V této části můžete nastavit automatické spouštění (a prioritu spouštění) transportního agenta. Na systémech Microsoft Exchange Server 2007 a novějších lze transportní agent nainstalovat pouze pokud je server v jedné z těchto dvou rolí: *Edge Transport* nebo *Hub Transport*.



POZNÁMKA: Transportní agent není ve verzii Microsoft Exchange Server 5.5. (VSAPI 1.0).

V menu **Nastavení priority agenta** můžete nastavovat priority agentů ESET Mail Security. Číselný rozsah priority agenta závisí na verzi Microsoft Exchange Server (čím je číslo nižší, tím je větší priorita).

Zapisovat stupeň nevyžádané pošty (SCL) do záhlaví kontrolovaných zpráv podle hodnoty SPAM skóre - SCL je hodnota přidělena zprávě, která indikuje pravděpodobnost, že zpráva je spam (vyhodnocují se specifika záhlaví zprávy, předmětu, obsahu atd.). Hodnocení 0 znamená, že je velmi nepravděpodobné, aby byla konkrétní zpráva spam, zatímco hodnocení 9 zase upozorňuje na vysokou pravděpodobnost spamu. Hodnoty SCL lze dále zpracovávat technologií Intelligent Message Filter (nebo Content Filter Agent) systému Microsoft Exchange Server. Podrobnější informace naleznete v dokumentaci k Microsoft Exchange Server.

Možnost **Při smazání zprávy odeslat zamítavou SMTP odpověď**:

- Pokud je tato volba vypnuta, server pošle OK SMTP odpověď v znění '250 2.5.0 – Requested mail action okay, completed' odesilátelskému MTA (Mail Transfer Agent) a potom vykoná tzv. silent drop.

- Pokud je zapnuta, odesilátelskému MTA se pošle SMTP reject odpověď (SMTP zamítnuto). Odpověď můžete napsat v tomto formátu:

Primární kód odpovědi	Doplňkový kód stavu	Popis
250	2.5.0	Requested mail action okay, completed
451	4.5.1	Requested action aborted: local error in processing
550	5.5.0	Requested action not taken: mailbox unavailable

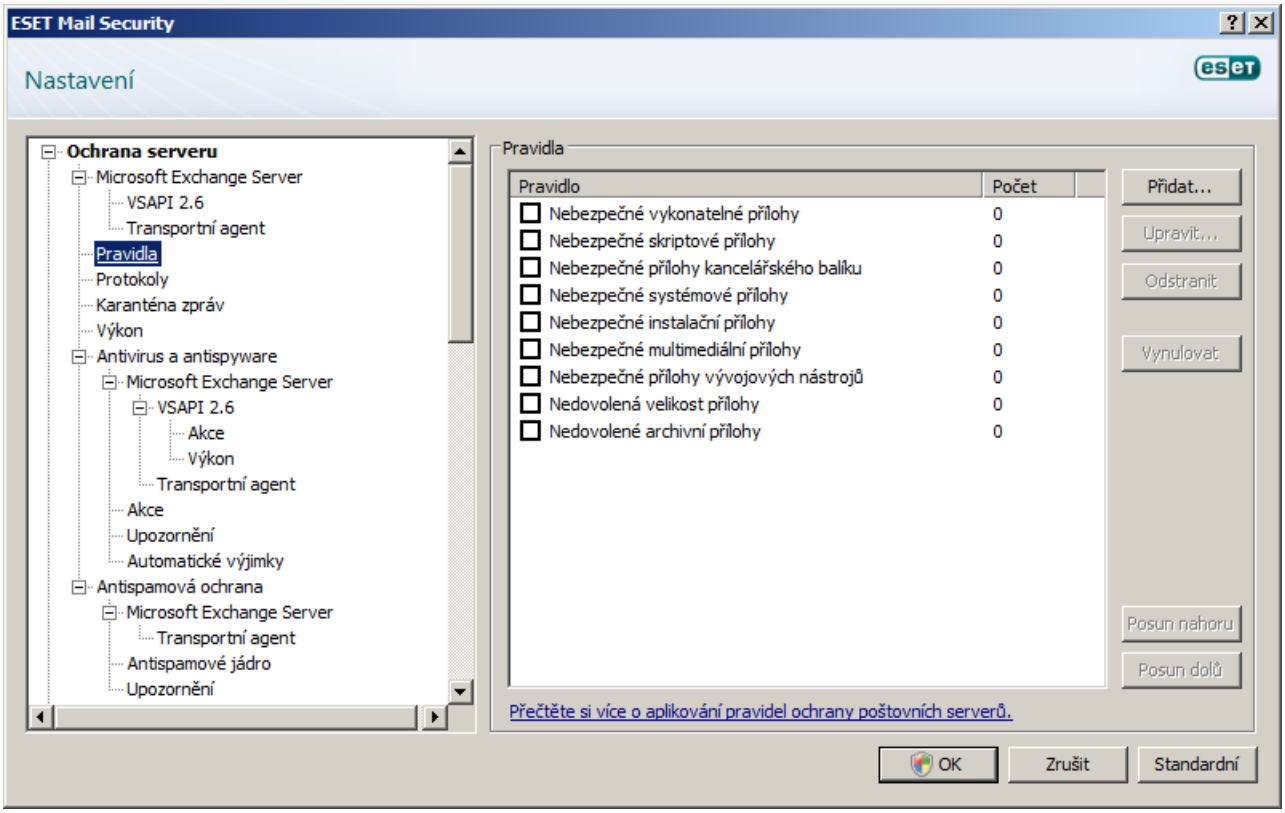
Upozornění: Použití nesprávné syntaxe v kódech odpovědí, může vést k znefunčkneniu programových komponent a snížení efektivity.

POZNÁMKA: Při nastavování SMTP Reject odpovědí můžete použít i systémové proměnné.

3.1.2 Pravidla

Pravidla umožňují administrátorům manuálně konfigurovat podmínky filtrování zpráv a také vybrat akce, které se s filtrovanými zprávami provedou. Pravidla se aplikují na základě definovaných podmínek. Více podmínek v rámci pravidla je kombinováno pomocí logického operátoru AND, přičemž pravidlo bude uplatněno pouze pokud jsou splněny všechny podmínky. Údaj ve sloupci **Počet** (vedle každého názvu pravidla) zobrazuje počet úspěšných použití pravidla.

Pravidla se porovnávají se zprávou při jejím zpracování transportním agentem (TA) nebo VSAPI. Pokud je povolena kontrola zpráv prostřednictvím TA i VSAPI, při příchodu zprávy se počítadlo pravidel může zvýšit io 2 nebo více. VSAPI přistupuje k jednotlivým částem zprávy (tělo, příloha) zvlášť a také pravidla jsou aplikovány na každou část zprávy zvlášť. Dále se pravidla používají i během kontroly na pozadí (např. opakovaná kontrola poštovní schránky po aktualizaci virové databáze), což rovněž přispívá ke zvyšování stavu počítadla.



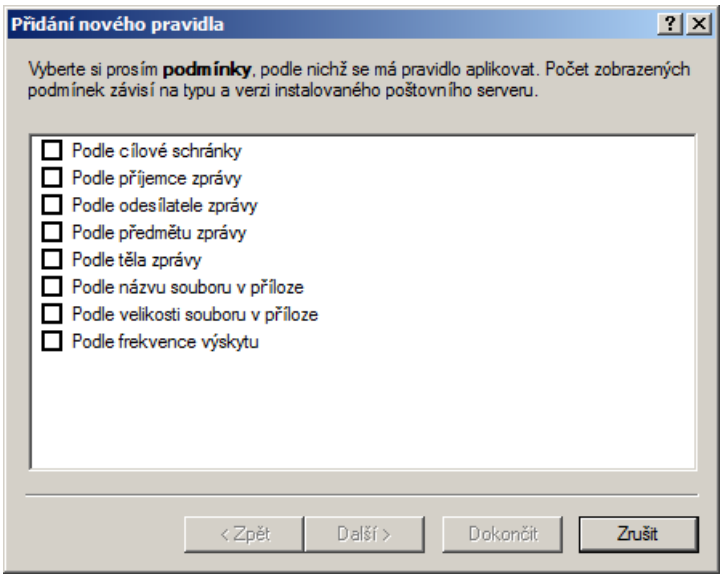
- **Přidat...** - umožní přidání nového pravidla
- **Upravit...** - umožní modifikaci existujícího pravidla
- **Odstranit** - odstraní vybrané pravidlo
- **Vynulovat** - vynuluje počítadlo konkrétního pravidla (sloupec **Počet**)
- **Posunout nahoru** - posune pravidlo výše
- **Posunout dolů** - posune pravidlo níže

Zrušením označení (zaškrtávací políčko vlevo od pravidla) spravidlo deaktivujete. Toto umožnuje znovu zapnout / aktivovat pravidlo v případě potřeby.

POZNÁMKA: Při použití pravidel se dají využít i systémové proměnné (např.:*% PATHEXT%*).

3.1.2.1 Přidání nového pravidla

Tento průvodce Vás provede přidáváním Vašich vlastních pravidel s kombinovanými podmínkami.



POZNÁMKA: Ne všechny podmínky jsou použitelné, pokud je zpráva kontrolována transportním agentem.

- **Podle cílové poštovní schránky** platí pre meno mailovej schránky (VSAPI)

- **Podle příjemce zprávy** platí pro zprávu poslanou specifickému příjemci (VSAPI + TA)
- **Podle odesílatele zprávy** platí pro zprávu poslanou od specifického odesílatele (VSAPI + TA)
- **Podle předmětu zprávy** platí pro zprávy se specifickým předmětem (VSAPI + TA)
- **Podle těla zprávy** platí pro zprávy se specifickým textem v těle zprávy (VSAPI)
- **Podle názvu souboru v příloze** platí pro zprávy se specifickým názvem přílohy (VSAPI)
- **Podle velikosti souboru v příloze** platí pro zprávy s velikostí přílohy přesahující definovanou velikost (VSAPI)
- **Podle frekvence výskytu** platí pro objekty (zprávy nebo přílohy) jejichž výskyt za nastavený čas přesáhne speficikovaný počet. Toto je obzvláště užitečné pokud Vám neustále přicházejí spamové zprávy se stejným tělem zprávy nebo stejnou přílohou (VSAPI + TA)

Při nastavování výše uvedených podmínek (kromě **Podle velikosti souboru v příloze**) stačí uvést pouze část fráze, pokud není zapnuta možnost **Porovnávat jako celá slova**. Pokud není zapnutá možnost Rozlišovat velikost písmen, tak velikost písmen se nebere ohled. Pokud používáte jiné hodnoty než alfanumerické znaky, použijte závorky a uvozovky. Při tvoření podmínek můžete použít i logické operátory AND, OR a NOT ("A", "NEBO" a "NE").

POZNÁMKA: Dostupnost jednotlivých pravidel je zavyslá od verze Microsoft Exchange Serveru.

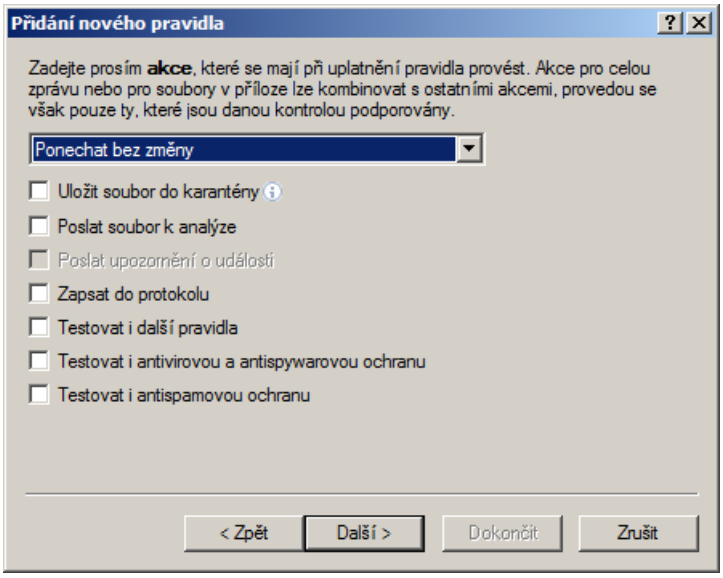
POZNÁMKA: Microsoft Exchange Server 2000 (VSAPI 2.0) hodnotí pouze zobrazované jméno příjemce / odesílatele, ne e-mailovou adresu. Vyhodnocování e-mailových adres je podporováno od verze Microsoft Exchange Server 2003 (VSAPI 2.5) a výše.

Príklady zadávania podmienok:

Podle cílové poštovní schránky	smith
Podle odesílatele zprávy	smith@mail.com
Podle příjemce zprávy	"J.Smith" or "smith@mail.com"
Podle předmětu zprávy:	" "
Podle názvu souboru v příloze:	".com" OR ".exe"
Podle těla zprávy:	("free" OR "lottery") AND ("win" OR "buy")

3.1.2.2 Akce

V této sekci můžete vybírat jaké akce budou provedeny se zprávami a / nebo přílohami, které spadají pod podmínky definované v pravidlech. Nemusíte provádět žádnou akci, můžete označit zprávu jako hrozbu / spam nebo zprávu zcela vymazat. V případě, že zpráva spadá do podmínek kteréhokoliv pravidla, nebude již kontrolovaná antivirem nebo antispamem, pokud není tato funkcionalita explicitně aktivována označením příslušného zaškrtávaciaho pole v dolní části okna (v takovém případě provedené akce závisí od antivirových / antispamových nastavení).



- **Ponechat bez změny** - neprovede se žádná akce
- **Označit jako neléčenou infiltraci** - označí zprávu stejně jako jako by obsahovala nevyléčenou infiltraci (nezávisle na tom, zda ji obsahuje)
- **Označit jako nevyžádanou poštu** - označí zprávu jako spam (bez ohledu na to, zda je či není spamem)
- **Smazat zprávu** - odstraní celou zprávu i s obsahem, pokud jsou splněny podmínky

- **Uložit soubor do karantény** uloží přiložený soubor do karantény

POZNÁMKA: Není shodné s karanténou e-mailových zpráv (viz. kapitola Karanténa zpráv 23).

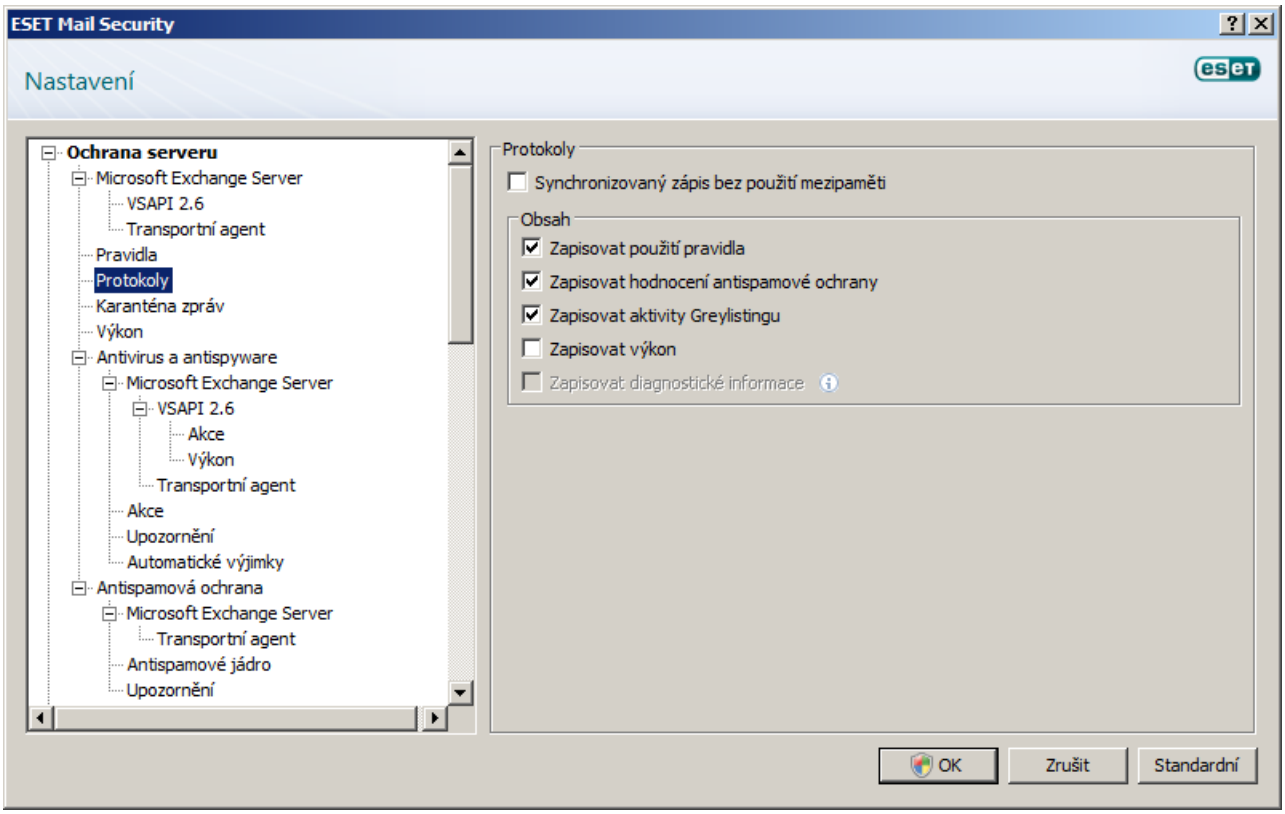
- **Poslat soubor k analýze** odešle podezřelé přílohy k analýze do virové laboratoře ESET
- **Poslat upozornění o události** pošle oznamení administrátorovi (v závislosti na nastavení v **Nastavení > Upozornění**).
- **Zapsat do protokolu** zapíše informaci o použitém pravidle do protokolu
- **Testovat i daší pravidla** povolí vyhodnocování dalších pravidel, čímž umožní uživateli nastavit více soustav podmínek a navazujících akcí.
- **Testovat i antivirovou a antispywarovou ochranou** zkontroluje zpávu i její přílohu
- **Testovat i anstispamovou ochranou** zkontroluje zprávu antispamovým modulem

POZNÁMKA: Tato možnost je dostupná pouze v systémech Microsoft Exchange Server 2OOO a novějších li zapnutý transportní agent.

Posledním krokem ve vytváření nového pravidla je pojmenování každého z vytvořených pravidel. Můžete přidat i komentář k pravidlu. Tato informace se uloží do protokolu Microsoft Exchange Serveru.

3.1.3 Protokoly

V nastavení protokolů si můžete upravit obsah, který se do souboru s protokolem bude zapisovat. Detailnější protokol obsahuje více informací, ale může mít negativní dopad na výkon serveru.



Pokud je zapnut **Synchronizovaný zápis bez použití vyrovnávací paměti**, všechny záznamy protokolu se hned zapíší do souboru, aniž byly nejprve uloženy ve vyrovnávací paměti. Standardně si komponenty ESET Mail Security, které běží pod systémem Microsoft Exchange Server, ukládají zprávy určené do protokolů do své interní paměti a posílají jejich aplikačnímu protokolu v pravidelných časových intervalech tak, aby nesnižovaly výkon serveru. Zde může nastat situace, kdy se nemusí zachovat chronologické integrita diagnostických záznamů v protokolu. Doporučujeme toto nastavení nezapínat, dokud to není nutné pro účely diagnostiky. V části **Obsah** můžete nastavit typy informací, které se budou do protokolů zapisovat.

- **Zapisovat použitá pravidla** - po zapnutí ESET Mail Security zapíše názvy všech zapnutých pravidel do souboru

- **Zapisovat hodnocení antispamové ochrany** - pokud máte zapnutou tuto volbu, pak bude aktivita týkající se nevyžádaných zpráv zapisována do Antispamového protokolu 79.V případě, že poštovní server přijme nevyžádanou zprávu (SPAM), informace o tom bude zapsána do protokolu s detaily jako je Čas / Datum, Odesílatel, Příjemce, Předmět, hodnocení antispamové ochrany (SPAM Score), Důvod a Akce provedená s

konkrétní nevyžádanou chovala . Toto je užitečné v případě, pokud potřebujete vysledovat jaké SPAM zprávy byly přijaty, zjistit kdy byly přijaty a jaká akce byla s těmito zprávami provedena.

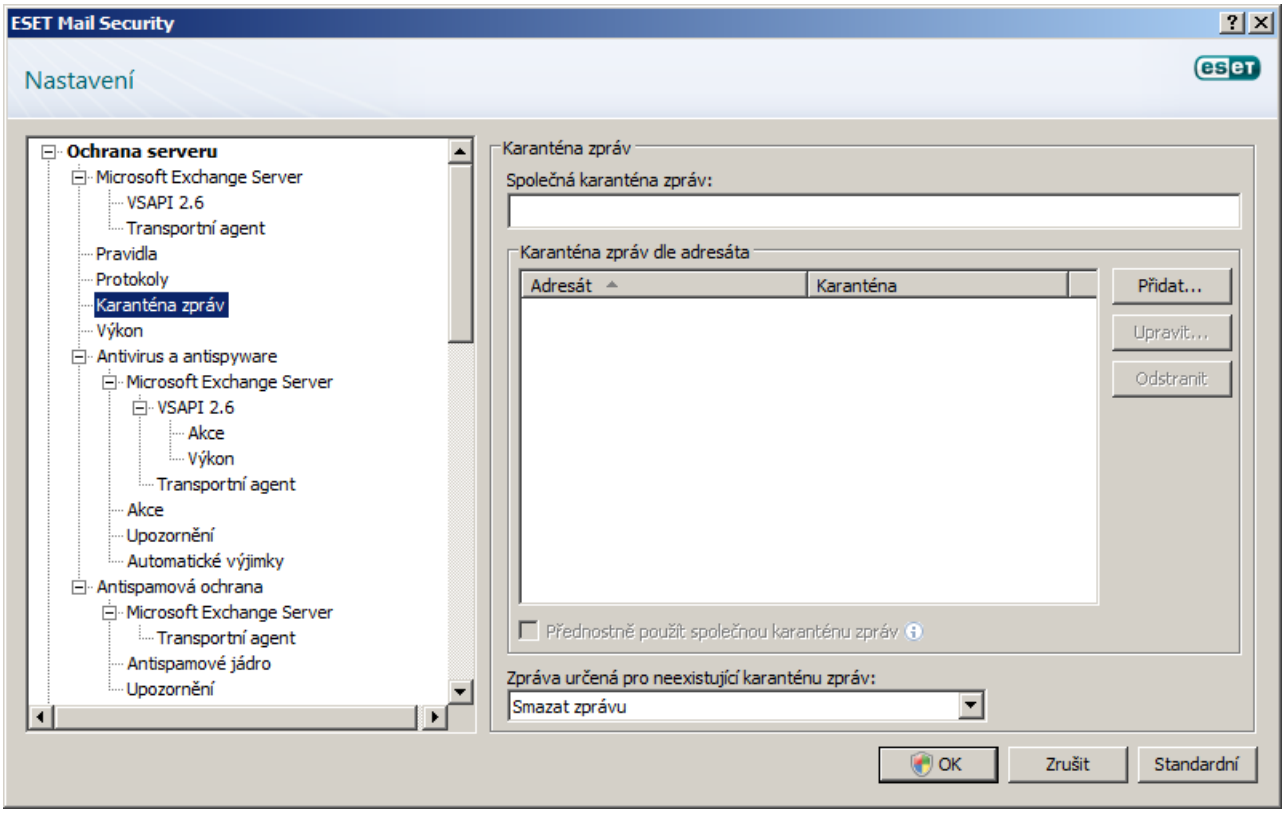
- **Zapisovat aktivity Greylistingu** - použijte tuto volbu, pokud si přejete, aby byly zápsány aktivity týkající se Greylistingu do protokolu Greylisting 79. Tento protokol poskytuje informacije jako je Čas / Datum, HELO Doména, IP adresa, Odesílatel, Příjemce, Akce, atd..
  POZNÁMKA: Tato volba funguje pouze v případě, že je funkce Greylisting zapnuta v možnostech Transportního agenta pod **Ochrana serveru** > **Antispamová ochrana** > **Microsoft Exchange Server** > **Transportní agent** ve stromu pokročilých nastavení (**F5**).

- **Zapisovat výkon** - zapíše informace o délce vykonané úkoly, velikosti kontrolovaného objektu, přenosové rychlosti (kb / s) a stavu výkonu.

- **Zapisovat diagnostické informace** - zaznamená diagnostické informace důležité pro ladění programu do protokolu; tato funkcionalita je užitečná zejména pro odstraňování chyb a problémů. Nedoporučujeme nechávat tuto možnost zapnutou, pokud to není nutné. Pro zobrazení informací poskytnutých touto funkcionalitou musíte nastavit minimální úroveň detailnosti protokolů na **Diagnostické záznamy** v menu rozšířených nastavení pod **Nástroje> Protokoly> Zaznamenávat události od úrovně**.

3.1.4 Karanténa zpráv

Karanténa zpráv je speciální poštovní schránka nastavena systémovým administrátorům, která slouží jako úložiště potenciálně infikovaných zpráv a spamu. Zprávy uložené v karanténě se dají analyzovat, případně i léčit pomocí novější virové databáze.



K dispozici máte možnost vybrat si kterou ze dvou druhů karantény budete používat pro potenciálně infikované zprávy a spam.

První možností je použít interní karanténu Microsoft Exchange serveru (toto platí pouze pro Microsoft Exchange Server 2007/2010). V tomto případě je použit interní mechanismus Exchange serveru na ukládání potenciálně infikovaných zpráv a spamu. V případě potřeby, vedle používání interní karantény Exchange serveru, můžete definovat ještě další samostatné schránky, které budou sloužit jako karanténě pro konkrétních příjemců. Toto znamená, že potenciálně infikované zprávy a spam, které byly původně určeny pro konkrétního příjemce, budou přesunuty do nadefinované schránky / karantény, místo toho, aby byly přesunuty do interní karantény Exchange serveru (která slouží jako obecná pro všechny ostatní spamy a potenciálně infikované zprávy) . To může být užitečné například pokud potřebujete mít při správě větší přehled nad potenciálně nakaženými zprávami a spamem.

Druhou možností je použít **Společnou karanténu zpráv**. V případě, že máte starší verzi Microsoft Exchange Serveru (5.5, 2000 or 2003), definujete **Společnou karanténu zpráv**, což je vlastně poštovní schránka, která bude použita jako úložiště potenciálně infikovaných zpráv a spamu. V tomto případě není použit interní systém Microsoft Exchange serveru. Místo toho je správcem systému určena specifická poštovní schránka pro všechny spamy a potenciálně infikované zprávy. Také je možnost nadefinovat několik poštovních schránek jako karanténa pro konkrétních příjemců. Výsledkem čehož je to, že se potenciálně infikované zprávy a spam budou rozdělovat do konkrétních karantény namísto toho, aby byly přesunuty do společné karantény zpráv. Rozdělovány jsou podle toho jak jsou definovány **Karanténa zpráv dle adresáta.**

- **Společná karanténa zpráv** - v tomto poli lze nastavit adresu karantény (např. hlavni_karantena@spolecnost.cz), nebo můžete použít interní karanténu Microsoft Exchange serveru (2007/2010) tak, že necháte toto pole prázdné a ve spodní části okna, v rozbalovacím menu, zvolíte možnosť **Uložit do systémové karantény zpráv poštovního serveru** (podmínkou je, že daná systémová karanténa Exchange servera je aktivní). Emaily jsou pak do této karantény přesouvány za použití vlastních nastavení vnitřního mechanismu Exchange serveru.
  POZNÁMKA: Exchange server standardně nemá aktivovanou interní karanténu zpráv. Pokud ji chcete aktivovat, je třeba otevřít Exchange Management Shell a zadat následující příkaz:

  Set-ContentFilterConfig -QuarantineMailbox nazev@domena.cz

  (nahraďte nazev@domena.cz skutečným názvem poštovní schránky, která bude použita Microsoft Exchange serverem jako jeho interní karanténa, např. exchangekarantena@spolecnost.cz)

- **Karanténa zpráv podle adresáta** - zde můžete nastavit několik karanténních adres pro více příjemců. Pravidla karanténa lze vypínat a zapínat podle potřeby označováním / rušením označení příslušných zaškrtávacích polí.

  Přidat... - ak chcete pridať nové pravidlo karantény, sem zadajte požadovanú e-mailovú adresu príjemcu a e-mailovú adresu karantény do ktorej sa bude presúvať pošta
  Upravit... - umožní upraviť vybrané pravidlo karantény
  Odstranit - vymaže vybrané pravidlo karantény
  Přednostně použít společnou karanténu zpráv - pokud je tato možnost zapnuta, zpráva se přesune do nastavené společné karantény v případě, že je splněno více než jedno z pravidel karantény (např. pokud má zpráva více příjemců a někteří z nich spadají pod několik pravidel karantény)

- **Zpráva určena pro neexistující karanténu zpráv:**

  Ponechat zprávu - ponechať správu aj napriek tomu, že bola označená ako spam.
  Smazat zprávu - zpráva bude vymazána za předpokladu, že je určena na příjemce, který nespadá pod žádné z pravidel karantény a není nastavena společná karanténa.
  Uložit do systémové karantény zpráv poštovního serveru - zpráva se uloží do karantény poštovního serveru (tato volba není dostupná ve verzi Microsoft Exchange Server 2003 a starších)

POZNÁMKA: Při změnách nastavení karantény můžete také používat systémové proměnné (např. *% USERNAME%*).

3.1.4.1 Přidání nového pravidla karantény

Zadejte požadovanou e-mailovou adresu příjemce a e-mailovou adresu karantény do příslušných polí.

Pokud chcete odstranit e-mailovou zprávu určenou pro příjemce, který nemá přiděleno karanténní pravidlo, označte v roletovém menu **Zpráva určená pro neexistující karanténu zpráv**: možnost **Smazat zprávu**.

3.1.5 Výkon

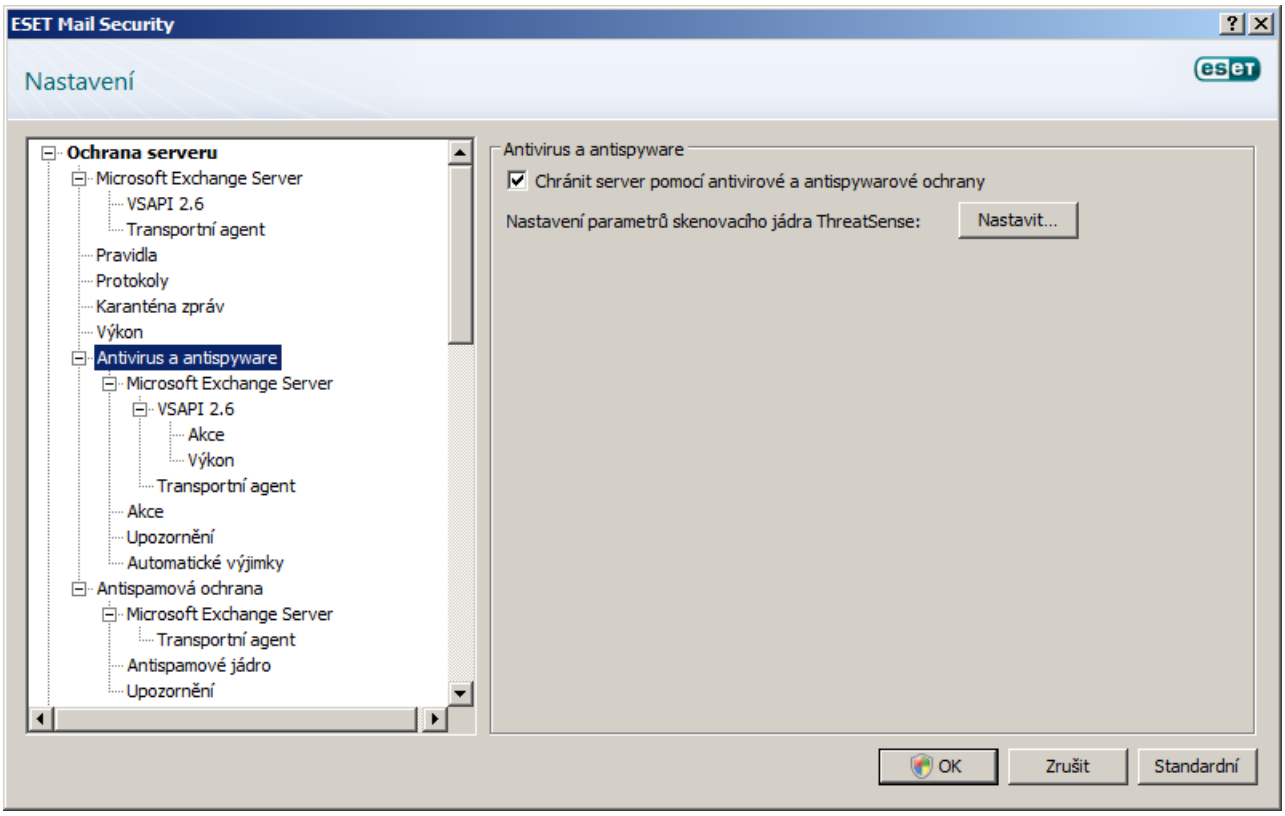
V této části můžete určit adresář, ve kterém se budou ukládat dočasné soubory, což umožňuje zvýšit výkon programu. Pokud nebyl určen žádný adresář, ESET Mail Security bude vytvářet dočasné soubory v dočasném systémovém adresáři.

POZNÁMKA: Pro účely minimalizace negativního vlivu ze roztříštěnosti a zpoždění při čtení a zápisu Vám doporučujeme dočasný adresář umístit na jiném harddisku než je Vaše instalace Microsoft Exchange Server. Doporučujeme vyhnout se ukládání dočasného adresáře na vyměnitelná média jako diskety, USB klíče, DVD atd..

POZNÁMKA: Při nastavování výkonu je možné používat systémové proměnné (např. *%SystemRoot%\TEMP*).

3.2 Nastavení antiviru a antispyware

Označním možnosti **Chrániť server pomocou antivírusovej a antispywarovej ochrany** zapnete antivírusovú a antispyware ochranu poštového servera. Antivírusová a antispyware ochrana sa zapnú vždy automaticky po každom reštarte servera/počítača. Kliknutím na tlačidlo **Nastaviť...** sa dostanete do nastavení parametrov skenovacieho jadra ThreatSense.



3.2.1 Microsoft Exchange Server

U antivirové a antispywarové ochrany používá <ESET Mail Security for Microsoft Exchange Server dva typy kontroly. Jeden typ využívá pro kontrolu zpráv VSAPI druhý zase transportního Agenta.

- Ochrana přes VSAPI 26 kontroluje zprávy přímo v úložišti zpráv Microsoft Exchange serveru.

- Ochrana přes transportního agenta 31 kontroluje zase přenos přes SMTP. Pokud je zapnutý tento druh ochrany, všechny zprávy spolu s jejich komponenty jsou kontrolovány ještě před jejich samotným doručením do úložiště zpráv Microsoft Exchange serveru, resp. před jejich odesláním přes SMTP. SMTP filtrování na úrovni serveru zajišťuje speciální plugin. U verzí Microsoft Exchange Server 2000 a 2003 se jedná o plugin Event Sink, který na SMTP serveru registrovaný jako součást IIS (Internet Information Services). Ve verzích Microsoft Server 2007 a 2010 je tento plugin registrován jako transportní agent na rolích Edge nebo Hub serveru Microsoft Exchange.

POZNÁMKA: Transportní agent není dostupný ve verzi Microsoft Exchange Server 5.5, najdete jej však ve všech novějších verzích Microsoft Exchange serveru (2000 a výše).

Antivirovou a antispywarovou ochranu pomocí VSAPI a transportního agenta můžete používat souběžně (je to

standardní a doporučené nastavení). Můžete se také rozhodnout pouze pro jeden z těchto druhů ochrany (buď VSAPI nebo Transportní agent). Tyto druhy ochrany umožňují nezávislou aktivaci resp. deaktivaci. Doporučujeme používat oba z těchto druhů antivirové a antispywarové ochrany. Nedoporučujeme nechávat oba druhy vypnuté.

3.2.1.1 Virus-Scanning Application Programming Interface (VSAPI)

Microsoft Exchange Server je vybaven mechanismem, který zajišťuje, že každá část zprávy se překontroluje nejnovější virovou databází. Pokud zpráva nebo její část ještě nebyla zkontrolována, tato bude oskenování dříve než se uvolní pro klienta. Každá podporovaná verze Microsoft Exchange Server (5.5/2000/2003/2007/2010) nabízí odlišnou verzi VSAPI.

3.2.1.1.1 Microsoft Exchange Server 5.5 (VSAPI 1.0)

Tato verze Microsoft Exchange Server obsahuje VSAPI verzi 1.0.

Možnost **Kontrolovat na pozadí** umožní kontrolu všech zpráv na pozadí systému. Microsoft Exchange Server si sám určuje, zda proběhne kontrola zpráv okamžitě nebo později, a to na základě různých faktorů jako jsou například momentálně zatížení serveru, počet aktivních uživatelů atd.. Microsoft Exchange Server si uchovává záznam o kontrolovaných zprávách a verzi virové databáze použité při skenování. Pokud se uživatel pokouší otevřít zprávu, která nebyla podrobena inspekci nejnovější verzí virových databází, Microsoft Exchange Server pošle zprávu nejprve na kontrolu ESET Mail Security a až potom ji umožní otevřít ve Vašem poštovním klientovi.

Protože kontrola na pozadí může zvýšit nároky na systém (kontrola probíhá po každé aktualizaci virové databáze), doporučujeme Vám používat plánovanou kontrolu mimo pracovní dobu. Plánovanou kontrolu na pozadí můžete nastavit přidáním úkoly v Plánovači. Pokud definujete úkol pro kontrolu na pozadí můžete určit čas spuštění, počet opakování a množství dalších parametrů dostupných v Plánovači. Naplánované úlohy se tato zobrazí v seznamu naplánovaných úloh, ve kterém ji také můžete upravovat, vymazat, nebo ji dočasně deaktivovat.

3.2.1.1.1.1 Akce

V této části můžete nastavit akce, které se provedou v případě, že zpráva a / nebo příloha byla vyhodnocena jako infikovaná.

Pole **Provést akci při neléčené infiltraci** určí, zda se škodlivý obsah zablokuje nebo se vymaže celá zpráva. Tato akce bude použita pouze pokud se při automatickém léčení (jak je definováno v **Nastavení parametrů skenovacího jádra ThreatSense** > Léčení 62) nepodařilo zprávu vyléčit.

Možnost **Smazání** umožnuje zredukovat velikost přílohy na nulovou hodnotu nebo nahradit infikovaný soubor virovým protokolem nebo názvem pravidla.

Akce

- **Vykonat akci při neléčené infiltraci:**
  - **Ponechat beze změny** - navzdory škodlivému obsahu se zprávou nebude provedena žádná akce
  - **Zablokovat** - zablokuje škodlivý obsah zprávy / přílohy
  - **Smazat** - vymaže zprávu se škodlivým obsahem

Smazání

- **Způsob smazání přílohy**
  - **Zkrátit soubor na nulovou délku** - ESET Mail Security zredukuje velikost přílohy na nulovou hodnotu a uživateli zobrazí název a typ souboru přílohy
  - **Nahradit přílohu informací o akci** - ESET Mail Security nahradí infikovaný soubor virovým protokolem nebo názvem pravidla

Kliknutím na **Opakovat** kontrolu program znovu posoudí i zprávy, které již byly testovány.

3.2.1.1.1.2 Výkon

Microsoft Exchange Server umožňuje během kontroly omezit čas na otevírání příloh zpráv. Tento čas se nastavuje v poli **Časový limit odezvy (v milisekundách):** a představuje dobu po které se klient znovu pokusí přistoupit k souboru, který předtím nebyl dostupný.

3.2.1.1.2 Microsoft Exchange Server 2000 (VSAPI 2.0)

Tato verze Microsoft Exchange Serveru obsahuje VSAPI verze 2.0

V případě, že vypnete možnost **Povolit antivirovou a antispywarovou ochranu VSAPI 2.0**, tak plug-in ESET Mail Security pro Exchange server nebude odebrán z procesu Microsoft Exchange serveru. Plug-in bude zprávy pouze propouštět bez kontroly na přítomnost virů. Přesto však budou zprávy kontrolovány na SPAM 35 a také budou aplikovány pravidla 19.

Pokud je zapnuta možnost **Proaktivní kontrola** nové příchozí zprávy budou kontrolovány v stejném pořadí jako byly přijaty. V případě, kdy uživatel otevře zprávu, která ještě nebyla zkontrolována, se tato zpráva zkontroluje předtím než jiné zprávy, které jsou zařazeny do kontroly.

Možnost **Kontrolovat na pozadí** umožní kontrolu všech zpráv na pozadí systému. Microsoft Exchange Server si sám určuje, zda proběhne kontrola zpráv okamžitě nebo později, a to na základě různých faktorů jako jsou například momentálně zatížení serveru, počet aktivních uživatelů atd. Microsoft Exchange Server si uchovává záznam o kontrolovaných zprávách a verzi virové databáze použité při skenování. Pokud se uživatel pokouší otevřít zprávu, která nebyla podrobena inspekci nejnovější virovou databází, Microsoft Exchange Server pošle zprávu nejprve na kontrolu ESET Mail Security zatímco ji umožní otevřít ve Vašem poštovním klientovi.

Protože kontrola na pozadí systému může zvýšit nároky na systém (kontrola probíhá po každé aktualizaci virové databáze), doporučujeme Vám používat plánovanou kontrolu mimo pracovní dobu. Plánovanou kontrolu na pozadí můžete nastavit přidáním úkoly v Plánovači. Pokud definujete úkol pro kontrolu na pozadí, můžete určit čas spuštění, počet opakování a množství dalších parametrů dostupných v Plánovači. Naplánované úlohy se tato zobrazí v seznamu naplánovaných úloh, ve kterém ji také můžete upravovat, vymazat, nebo ji dočasně deaktivovat.

Pokud chcete aby byly kontrolovány zprávy s prostým textem zaškrtněte možnost **Kontrolovat těla textových zpráv**.

Pokud povolíte možnost **Kontrolovat těla RTF zpráv** zapne se kontrola těl RTF zpráv.

3.2.1.1.2.1 Akce

V této části můžete nastavit akce, které se provedou v případě, že zpráva a/ nebo příloha byla vyhodnocena jako infikovaná.

Pole **Provést akci při neléčené infiltraci** určí, zda se škodlivý obsah zablokuje nebo se vymaže celá zpráva. Tato akce bude použita pouze pokud se při automatickém léčení (jak je definováno v **Nastavení parametrů skenovacího jádra ThreatSense** > Léčení 62) nepodařilo zprávu vyléčit.

Následují možnosti akcí, které lze provést (**Vykonat akci při neléčené infiltraci**):

- **Ponechat beze změny** - navzdory škodlivému obsahu se zprávou nebude provedena žádná akce
- **Zablokovat** - zablokuje škodlivý obsah zprávy / přílohy
- **Smazat** - vymaže zprávu se škodlivým obsahem

Možnost **Způsob mazání těla zprávy** nabízí alternativu, která spočívá v smazání těla zprávy nebo další, která přepíše tělo zprávy informací o provedené akci.

- **Smazat tělo zprávy** - vymaže tělo infikované zprávy; příjemci bude doručena prázdná zpráva a nezasažená přílohy
- **Přepsat tělo zprávy informací o akci** - přepíše tělo zprávy informací o provedené akci / akcích.

Způsob smazání přílohy určuje, zda se vymaže celá zpráva, nebo se redukuje velikost přílohy na nulu, nebo se infikovaný soubor nahradí informacemi o provedené akci.

- **Zkrátit soubor na nulovou délku** - ESET Mail Security zredukuje velikost přílohy na nulovou hodnotu a uživateli zobrazí název a typ souboru přílohy
- **Nahradit přílohu informací o akci** - ESET Mail Security nahradí infikovaný soubor virovým protokolem nebo názvem pravidla

Kliknutím na **Opakovat** kontrolu program znovu posoudí i zprávy, které již byly testovány.

3.2.1.1.2.2 Výkon

V této sekci můžete měnit počet nezávislých vláken kontroly, které mohou být najednou použity. Použití více vláken na systémech s více procesory může zvýšit rychlost kontroly. Pro co najvhodnešie optimalizování výkonu doporučujeme použít tolik skenovacích jader Technologii ThreatSense kolik použijeme skenovacích vláken.

Možnost **Časový limit odezvy (v sekundách)**: definuje maximální časový úsek, v jehož rámci vlákno čeká na dokončení kontroly zprávy. Pokud není skenování dokončeno v tomto časovém limitu, Microsoft Exchange Server odmítne klientovi přístup ke zprávě. Skenování přitom není přerušeno a po jeho dokončení bude každý další pokus klienta o přístup k této zprávě úspěšný.

TIP: Pro určení optimální hodnoty **Počet vláken kontroly**, dodavatel Microsoft Exchange Server doporučuje použít vzorec: [počet fyzických procesorů] x 2 + 1.

POZNÁMKA: Výkon se nezvýší, pokud je nastaveno více skenovacích jader ThreatSense jako skenovacích vláken.

3.2.1.1.3 Microsoft Exchange Server 2003 (VSAPI 2.5)

Táto verzia Microsoft Exchange Server v sebe zahŕňa VSAPI verziu 2.5.

V případě, že vypnete možnost **Povolit antivirovou a antispywarovou ochranu VSAPI 2.5**, tak plug-in ESET Mail Security pro Exchange server nebude odebrán z procesu Microsoft Exchange serveru. Plug-in bude zprávy pouze propouštět bez kontroly na přítomnost virů. Přesto však budou zprávy kontrolovány na SPAM 35 a také budou aplikovány pravidla 19.

Pokud je zapnuta možnost **Proaktivní kontrola** nové příchozí zprávy budou kontrolovány v stejném pořadí jako byly přijaty. V případě pokud uživatel otevře zprávu která ještě nebyla zkontrolována, tato zpráva se zkontroluje předtím než jiné zprávy, které jsou zařazeny do kontroly.

Možnost **Kontrolovat na pozadí** umožní kontrolu všech zpráv na pozadí systému. Microsoft Exchange Server si sám určuje, zda proběhne kontrola zpráv okamžitě nebo později, a to na základě různých faktorů jako jsou například momentálně zatížení serveru, počet aktivních uživatelů atd. Microsoft Exchange Server si uchovává záznam o kontrolovaných zprávách a verzi virové databáze použité při skenování. Pokud se uživatel pokouší otevřít zprávu, která nebyla podrobena inspekci nejnovější virovou databází, Microsoft Exchange Server pošle zprávu nejprve na kontrolu ESET Mail Security zatímco ji umožní otevřít ve Vašem poštovním klientovi.

Protože kontrola na pozadí systému může zvýšit nároky na systém (kontrola probíhá po každé aktualizaci virové databáze), doporučujeme Vám používat plánovanou kontrolu mimo pracovní dobu. Plánovanou kontrolu na pozadí můžete nastavit přidáním úkoly v Plánovači. Pokud definujete úkol pro kontrolu na pozadí, můžete určit čas spuštění, počet opakování a množství dalších parametrů dostupných v Plánovači. Naplánované úlohy se tato zobrazí v seznamu naplánovaných úloh, ve kterém ji také můžete upravovat, vymazat, nebo ji dočasně deaktivovat.

Pokud povolíte možnost **Kontrolovat těla RTF zpráv** zapne se kontrola těl RTF zpráv.

Možnost **Kontrolovat těla textových zpráv** zapne funkcionalitu, která zkontroluje i zprávy, které se neukládají na lokálním Microsoft Exchange Serveru, ale jsou přes něj jen doručovány jiným poštovním serverem. Pokud je zapnuta kontrola procházejících zpráv jejich také zkontroluje. Tato možnost je dostupná pouze pokud je vypnutý transportní agent.

POZNÁMKA: VSAPI nekontroluje těla textových zpráv (Plain Text).

3.2.1.1.3.1 Akce

V této části můžete nastavit akce, které se provedou v případě, že zpráva a/ nebo příloha byla vyhodnocena jako infikovaná.

Pole **Provést akci při neléčené infiltraci** určí, zda se škodlivý obsah zablokuje nebo se vymaže celá zpráva. Tato akce bude použita pouze pokud se při automatickém léčení (jak je definováno v **Nastavení parametrů skenovacího jádra ThreatSense** > Léčení 62) nepodařilo zprávu vyléčit.

Následují možnosti akcí, které lze provést (**Vykonat akci při neléčené infiltraci**):

- **Ponechat beze změny** - navzdory škodlivému obsahu se zprávou nebude provedena žádná akce
- **Zablokovat** - zablokuje škodlivý obsah zprávy / přílohy
- **Smazat** - vymaže zprávu se škodlivým obsahem

Možnost **Způsob mazání těla zprávy** nabízí alternativu, která spočívá v smazání těla zprávy nebo další, která přepíše tělo zprávy informací o provedené akci.

- **Smazat tělo zprávy** - vymaže tělo infikované zprávy; příjemci bude doručena prázdná zpráva a nezasažená přílohy
- **Přepsat tělo zprávy informací o akci** - přepíše tělo zprávy informací o provedené akci / akcích.

Způsob smazání přílohy určuje, zda se vymaže celá zpráva, nebo se redukuje velikost přílohy na nulu, nebo se infikovaný soubor nahradí informacemi o provedené akci.

- **Zkrátit soubor na nulovou délku** - ESET Mail Security zredukuje velikost přílohy na nulovou hodnotu a uživateli zobrazí název a typ souboru přílohy
- **Nahradit přílohu informací o akci** - ESET Mail Security nahradí infikovaný soubor virovým protokolem nebo názvem pravidla

Kliknutím na **Opakovat** kontrolu program znovu posoudí i zprávy, které již byly testovány.

3.2.1.1.3.2 Výkon

V této sekci můžete měnit počet nezávislých vláken kontroly, které mohou být najednou použity. Použití více vláken na systémech s více procesory může zvýšit rychlost kontroly. Pro co najvhodnešie optimalizování výkonu doporučujeme použít tolik skenovacích jader Technologii ThreatSense kolik použijeme skenovacích vláken.

Možnost **Časový limit odezvy (v sekundách)**: definuje maximální časový úsek, v jehož rámci vlákno čeká na dokončení kontroly zprávy. Pokud není skenování dokončeno v tomto časovém limitu, Microsoft Exchange Server odmítne klientovi přístup ke zprávě. Skenování přitom není přerušeno a po jeho dokončení bude každý další pokus klienta o přístup k této zprávě úspěšný.

TIP: Pro určení optimální hodnoty **Počet vláken kontroly**, dodavatel Microsoft Exchange Server doporučuje použít vzorec: [počet fyzických procesorů] x 2 + 1.

POZNÁMKA: Výkon se nezvýší, pokud je nastaveno více skenovacích jader ThreatSense jako skenovacích vláken.

3.2.1.1.4 Microsoft Exchange Server 2007/2010 (VSAPI 2.6)

Tato verze Microsoft Exchange Server obsahuje VSAPI verze 2.6.

V případě, že vypnete možnost **Povolit antivirovou a antispywarovou ochranu VSAPI 2.6**, tak plug-in ESET Mail Security pro Exchange server nebude odebrán z procesu Microsoft Exchange serveru. Plug-in bude zprávy pouze propouštět bez kontroly na přítomnost virů. Přesto však budou zprávy kontrolovány na SPAM 35 a také budou aplikovány pravidla 19.

Pokud je zapnuta možnost **Proaktivní kontrola** nové příchozí zprávy budou kontrolovány v stejném pořadí jako byly přijaty. V případě pokud uživatel otevře zprávu která ještě nebyla zkontrolována, tato zpráva se zkontroluje předtím než jiné zprávy, které jsou zařazeny do kontroly.

Možnost **Kontrolovat na pozadí** umožní kontrolu všech zpráv na pozadí systému. Microsoft Exchange Server si sám určuje, zda proběhne kontrola zpráv okamžitě nebo později, a to na základě různých faktorů jako jsou

například momentálně zatížení serveru, počet aktivních uživatelů atd. Microsoft Exchange Server si uchovává záznam o kontrolovaných zprávách a verzi virové databáze použité při skenování. Pokud se uživatel pokouší otevřít zprávu, která nebyla podrobena inspekci nejnovější virovou databází, Microsoft Exchange Server pošle zprávu nejprve na kontrolu ESET Mail Security zatímco ji umožní otevřít ve Vašem poštovním klientovi. Můžete rovněž zvolit možnost **Kontrolovat jen zprávy s přílohou** a filtrovat jejich podle času kdy byly přijaty:

- **Všechny zprávy**
- **Zprávy přijaté za poslední rok**
- **Zprávy přijaté za poslední půlrok**
- **Zprávy přijaté za poslední čtvrtrok**
- **Zprávy přijaté za poslední měsíc**
- **Zprávy přijaté za poslední týden**

Protože kontrola na pozadí systému může zvýšit nároky na systém (kontrola probíhá po každé aktualizaci virové databáze), doporučujeme Vám používat plánovanou kontrolu mimo pracovní dobu. Plánovanou kontrolu na pozadí můžete nastavit přidáním úkoly v Plánovači. Pokud definujete úkol pro kontrolu na pozadí, můžete určit čas spuštění, počet opakování a množství dalších parametrů dostupných v Plánovači. Naplánované úlohy se tato zobrazí v seznamu naplánovaných úloh, ve kterém ji také můžete upravovat, vymazat, nebo ji dočasně deaktivovat.

Pokud povolíte možnost **Kontrolovat těla RTF zpráv** zapne se kontrola těl RTF zpráv.

POZNÁMKA: VSAPI nekontroluje těla textových zpráv (Plain Text).

3.2.1.1.4.1 Akce

V této části můžete nastavit akce, které se provedou v případě, že zpráva a/ nebo příloha byla vyhodnocena jako infikovaná.

Pole **Provést akci při neléčené infiltraci** určí, zda se škodlivý obsah zablokuje nebo se vymaže celá zpráva. Tato akce bude použita pouze pokud se při automatickém léčení (jak je definováno v **Nastavení parametrů skenovacího jádra ThreatSense** > Léčení 62) nepodařilo zprávu vyléčit.

Následují možnosti akcí, které lze provést (**Vykonat akci při neléčené infiltraci**):

- **Ponechat beze změny** - navzdory škodlivému obsahu se zprávou nebude provedena žádná akce
- **Zablokovat** - zablokuje škodlivý obsah zprávy / přílohy
- **Smazat objekt** - vymaže škodlivý obsah zprávy
- **Smazat celou zprávu** - vymaže celou zprávu včetně škodlivého obsahu

Možnost **Způsob mazání těla zprávy** nabízí alternativu, která spočívá v smazání těla zprávy nebo další, která přepíše tělo zprávy informací o provedené akci.

- **Smazat tělo zprávy** - vymaže tělo infikované zprávy; příjemci bude doručena prázdná zpráva a nezasažená přílohy
- **Přepsat tělo zprávy informací o akci** - přepíše tělo zprávy informací o provedené akci / akcích.
- **Smazat celou zprávu** - vymaže celou zprávu včetně škodlivého obsahu a příloh

Způsob smazání přílohy určuje, zda se vymaže celá zpráva, nebo se redukuje velikost přílohy na nulu, nebo se infikovaný soubor nahradí informacemi o provedené akci.

- **Zkrátit soubor na nulovou délku** - ESET Mail Security zredukuje velikost přílohy na nulovou hodnotu a uživateli zobrazí název a typ souboru přílohy
- **Nahradit přílohu informací o akci** - ESET Mail Security nahradí infikovaný soubor virovým protokolem nebo názvem pravidla
- **Smazat celou zprávu** - vymaže přílohu

Pokud je zapnuta možnost **Použít karanténu VSAPI**, infikované zprávy budou ukládat do karantény poštovního serveru. Zde je třeba upozornit na fakt, že toto je serverem spravována karanténa a ne karanténa klienta, ani poštovní složku karantény. Infikované zprávy uložené v karanténě poštovního serveru nejsou dostupné, dokud nejsou vyléčeny pomocí nově aktualizované virové databáze.

Kliknutím na **Opakovat kontrolu** program znovu posoudí i zprávy, které již byly testovány.

3.2.1.1.4.2 Výkon

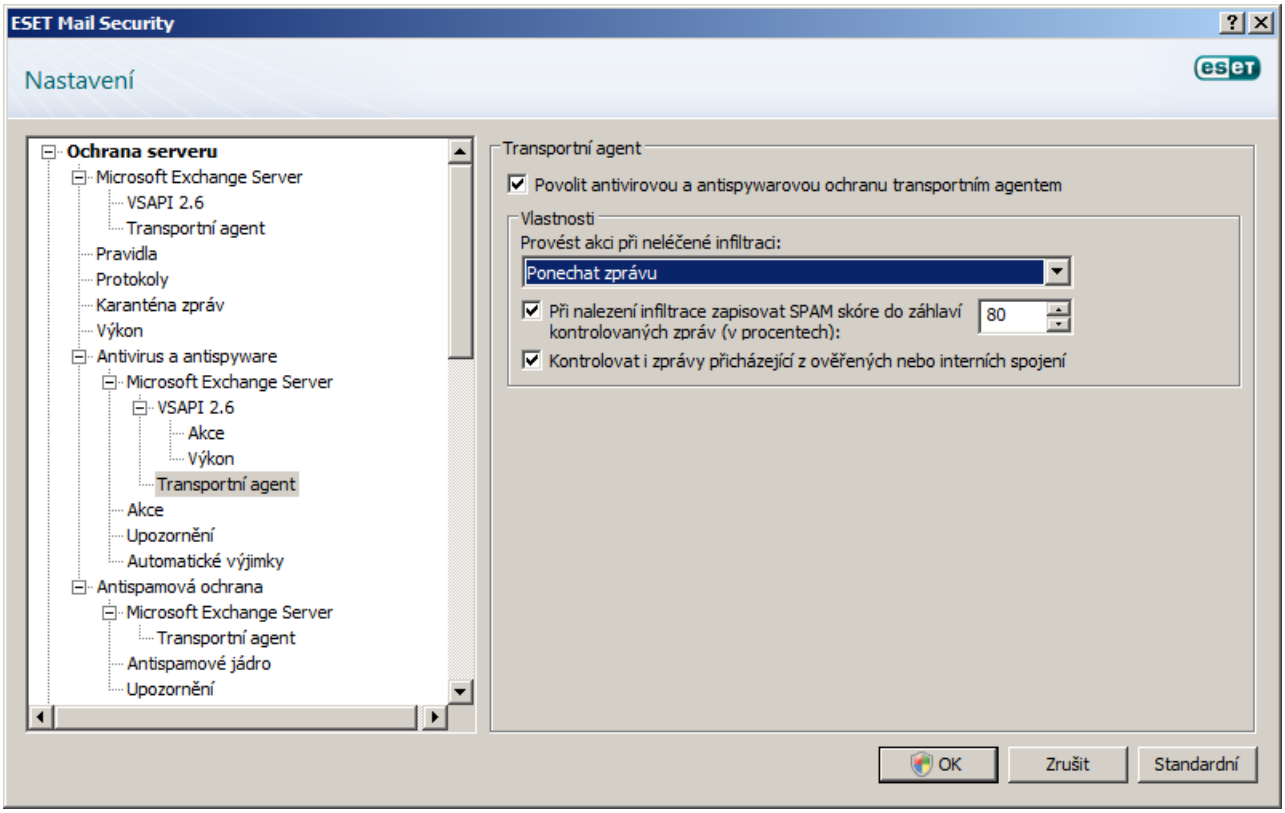
V této sekci můžete měnit počet nezávislých vláken kontroly, které mohou být najednou použity. Použití více vláken na systémech s více procesory může zvýšit rychlost kontroly. Pro co najvhodnešie optimalizování výkonu doporučujeme použít tolik skenovacích jader Technologii ThreatSense kolik použijeme skenovacíh vláken.

TIP: Pro určení optimální hodnoty **Počet vláken kontroly**, dodavatel Microsoft Exchange Server doporučuje použít vzorec: [počet fyzických procesorů] x 2 + 1.

POZNÁMKA: Výkon se nezvýší, pokud je nastaveno více skenovacích jader ThreatSense jako skenovacích vláken.

3.2.1.2 Transportní Agent

V této části můžete zapnout antivirovou a antispywarovou ochranu transportním agentem. Transportní agent pro Microsoft Exchange Server 2007 a výše se dá nainstalovat pouze v případě, že server je v jedné z těchto dvou rolí: *Edge Transport* nebo *Hub Transport*.



Pokud se zpráva nedá vyléčit, bude dále zpracována podle nastavení v sekci Transportní Agent. Zpráva může být vymazána, přesunuta do karantény nebo zachována.

V případě, že vypnete možnost **Povolit antivirovou a antispywarovou ochranu VSAPI**, tak plug-in ESET Mail Security pro Exchange server nebude odebrán z procesu Microsoft Exchange serveru. Plug-in bude zprávy pouze propouštět bez kontroly na přítomnost virů. Přesto však budou zprávy kontrolovány na SPAM 35 a také budou aplikovány pravidla 19.

Pokud aktivujete možnost **Povolit antivirovou a antispywarovou ochranu transportním agentem**, tak máte možnost nastavit následující akce, které se provedou při neléčených infiltracích (**Provést akci při neléčené infiltraci**):

Ponechat zprávu - zachová zprávu, která nebyla vyléčena
Přesunout zprávu do karantény - přesune infikovanou zprávu do schránky karantény
Smazat zprávu - vymaže infikovanou zprávu

Při nalezení infiltrace zapisovat SPAM skóre do záhlaví kontrolovaných zpráv (v procentech): - zde nastavte spam skóre (pravděpodobnost že zpráva je spam) v procentech

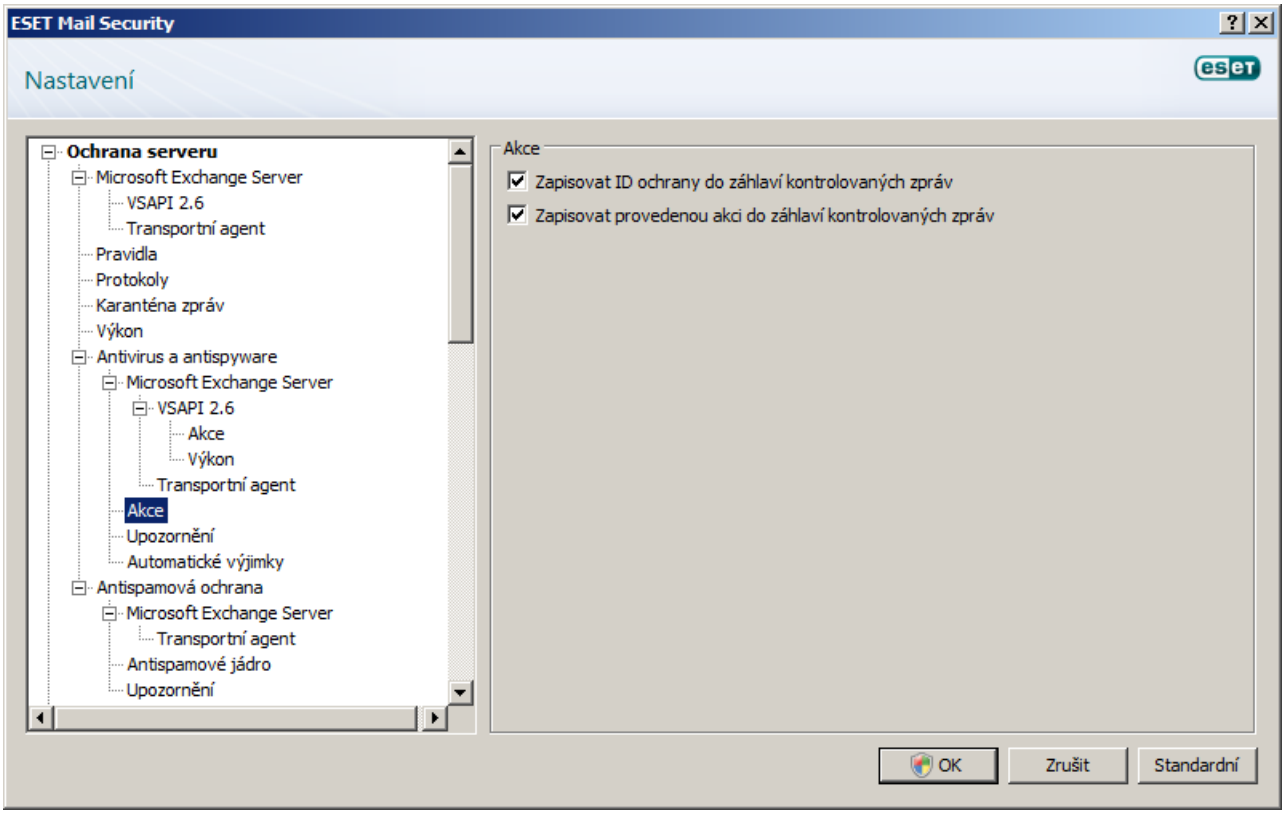
Toto znamená, že pokud byla nalezena infiltrace, můžete kontrolované zprávě připsat spam skóre, jehož hodnotu

udáváte v procentech. Že botnety jsou dnes absolutně většinovým vlastníkem odesílatelům infikované pošty, zprávy posílané tímto způsobem mohou být klasifikovány jako spam. Aby tato funkcionalita mohla správně fungovat, musí být zapnuta volba **Zapisovat stupeň nevyžádané pošty (SCL) do záhlaví kontrolovaných zpráv podle hodnoty SPAM skóre** v části **Ochrana serveru> Microsoft Exchange Server>** Transportní agent 18.

Pokud je možnost **Kontrolovat i zprávy přicházející z totožností nebo interních spojení** povolena, tak se budou kontrolovat i zprávy přicházející z totožností zdrojů nebo lokálních serverů.

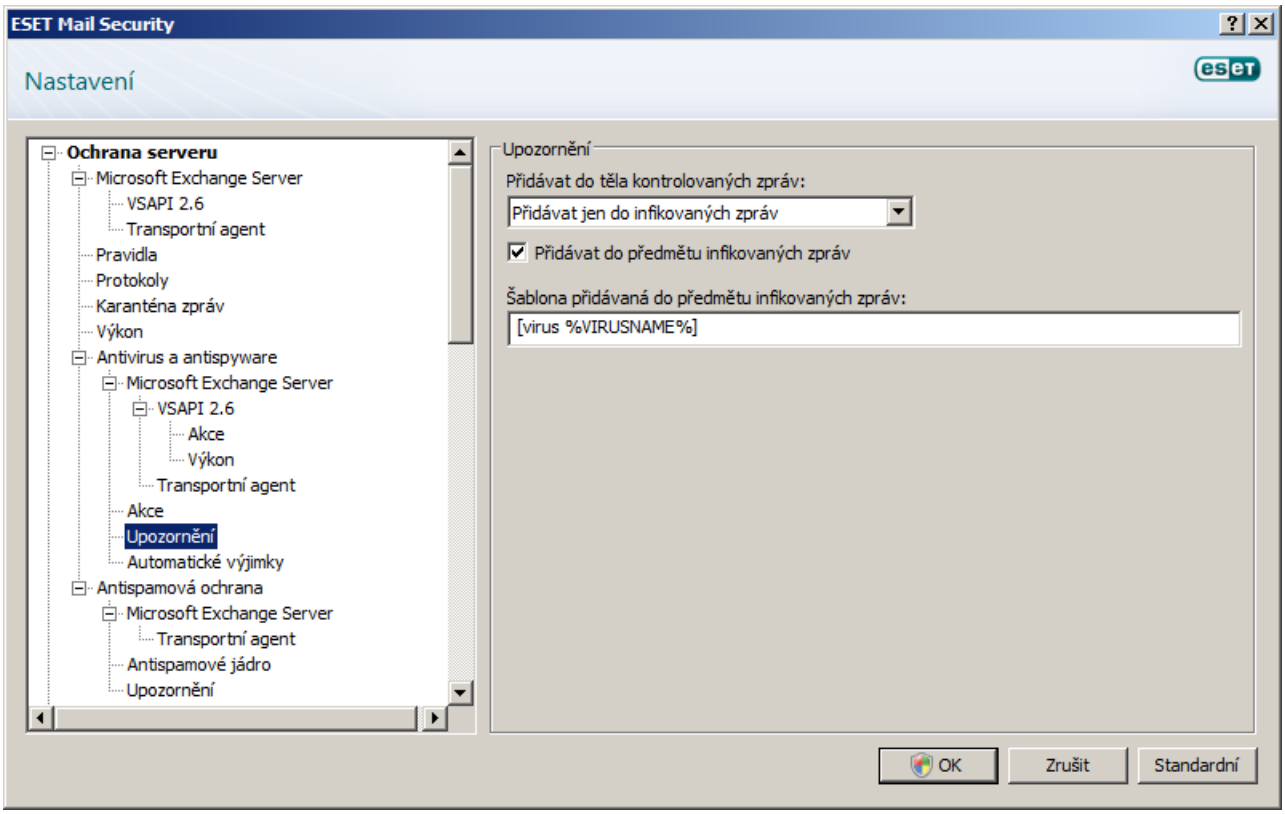
3.2.2 Akce

V této sekci můžete zapnout přidávání ID kódu skenovací úkoly a také provedené akce do záhlaví kontrolovaných zpráv.



3.2.3 Upozornění

ESET Mail Security Vám nabízí možnost přidávat text k původnímu předmětu, nebo přímo do těla infikovaných zpráv.



Přidávat do těla kontrolovaných zpráv: nabízí tři možnosti:

- Nepřidávat do zpráv
- Přidávat jen do infikovaných zpráv
- Přidávat do všech kontrolovaných zpráv

Pokud zapnete možnost **Přidávat do předmětu infikovaných zpráv**, ESET Mail Security přidá do předmětu e-mailové zprávy text definovaný v textovém poli **Šablona přidávaná do předmětu infikovaných zpráv**: (přednastavené je [virus% VIRUSNAME%]). Výše nastavení mohou automatizovat filtrování infikovaných zpráv tříděním zpráv do vlastních adresářů podle slov v předmětu zprávy (pokud tuto funcionalitu podporuje váš poštovní klient).

POZNÁMKA: Při sestavování textu, který se přidá do předmětu zprávy můžete použít i systémové proměnné.

3.2.4 Automatické výjimky

Pro většinu serverových aplikací/ operačních systémů doporučují jejich výrobci celé sady výjimek pracovních souborů a složek z kontroly antivirovým programem. Je to zejména kvůli tomu, že antivirová kontrola těchto důležitých součástí může mít nepříznivý vliv na výkon serveru a může dokonce způsobit konflikty vedoucí k nefunkčnost serverové aplikace. Tyto výjimky přispívají k rychlejšímu chodu serveru a minimalizují riziko potenciálních konfliktů.

ESET Mail Security detekuje nainstalované serverové aplikace/ operační systém a automaticky je zařazuje do seznamu Výjimek. Aplikace/ operační systém v sezname lze aktivovat zaškrtnutím (standardní nastavení), nebo deaktivováním-odškrtnutím (zásahem uživatele), přičemž výjimky se v těchto případech aplikují následovně:

1) Pokud je aplikace/ operační systém v seznamu aktivována, do vyloučení ze skenování antivirovou ochranou (**Pokročilé nastavení** > **Ochrana počítače** > **Antivirus a antispyware** > **Výjimky**) budou přidány kritické soubory a složky dané aplikace, přičemž jejich přítomnost ve výjimkách je po každém restartu serveru kontrolována a v případě vymazání některé výjimky, dojde k jejímu opětovnému zařazení. Tuto variantu doporučujeme, pokud si chcete být vždy jisti, že doporučené výjimky jsou aplikovány.

2) Pokud některou aplikaci/ operační systém ze seznamu uživatel deaktivuje, její kritické soubory a složky stále zůstanou ve výjimkách ze skenování antivirovou ochranou (**Pokročilé nastavení** > **Ochrana počítače** > **Antivirus a antispyware** > **Výjimky**), nebude přítomnost souborů ve výjimkách kontrolována ani obnovena. Tato varianta je doporučena zkušenějším uživatelům.

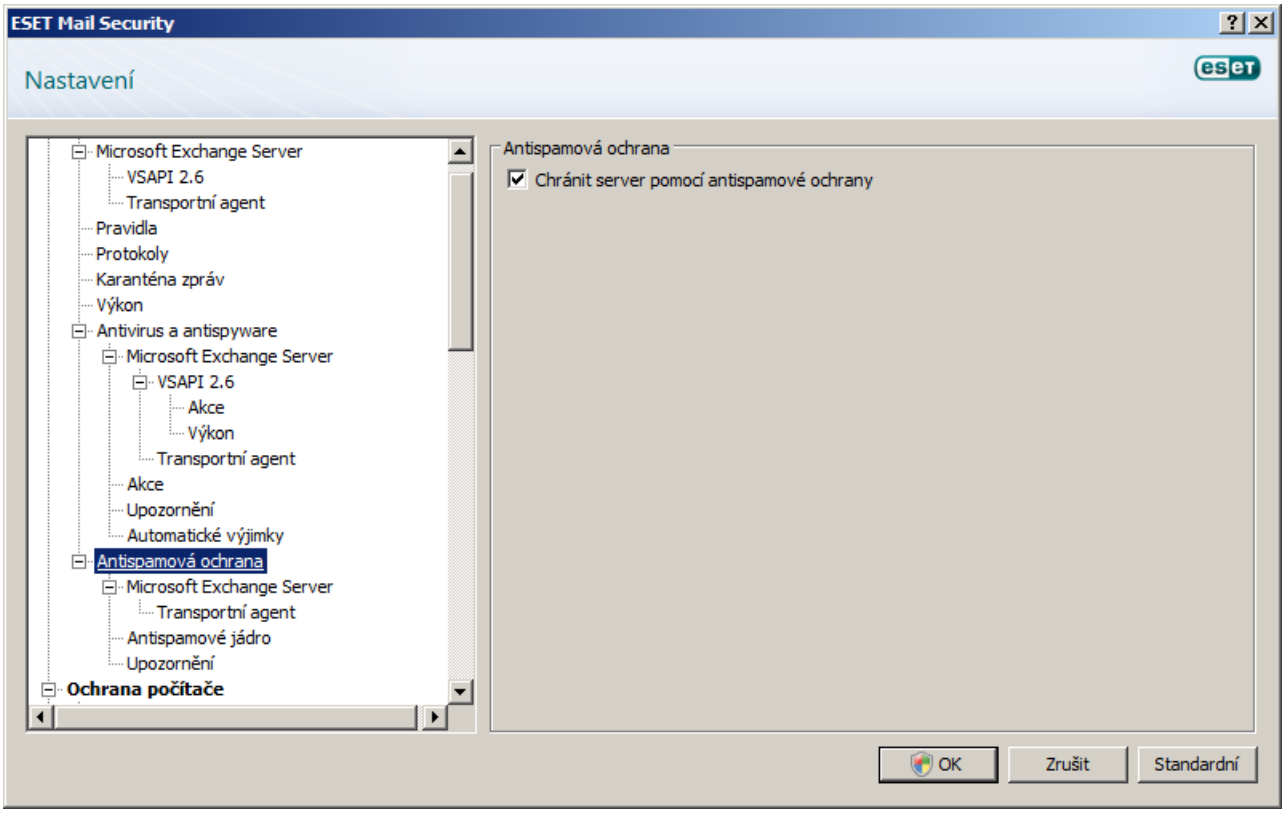
Ostatní uživatelem přímo zadané výjimky v **Pokročilé nastavení** > **Ochrana počítače** > **Antivirus a antispyware** > **Výjimky** nejsou výše uvedeným nastavení nijak ovlivněny.

Výjimky pro jednotlivé serverové aplikace/ operační systémy vycházejí z doporučeného nastavení společnosti Microsoft. Např.

http://support.microsoft.com/kb/822158
http://support.microsoft.com/kb/245822
http://support.microsoft.com/kb/823166
http://technet.microsoft.com/en-us/library/bb332342%28EXCHG.80%29.aspx
http://technet.microsoft.com/en-us/library/bb332342.aspx

3.3 Antispamová ochrana

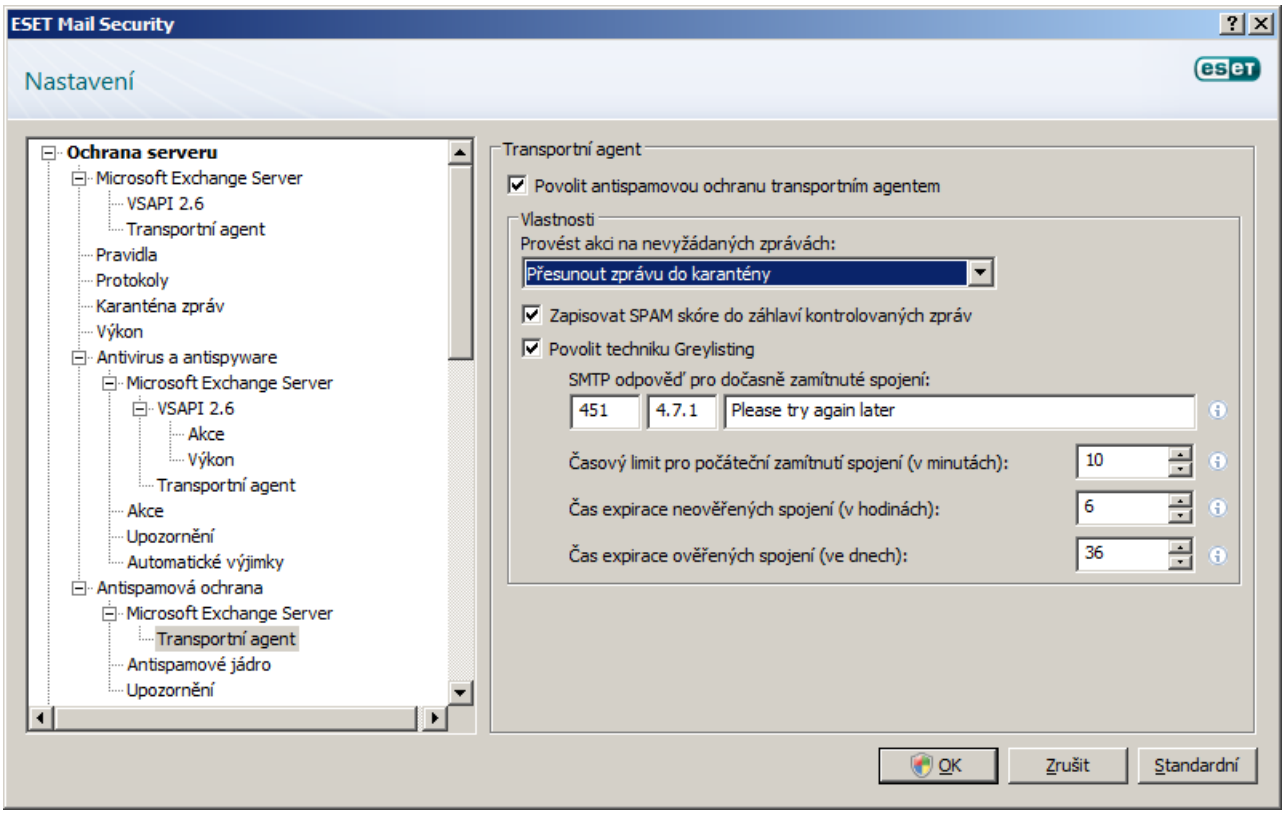
V sekci **Antispamová ochrana** můžete zapnout ochranu proti spamu na vašem poštovním serveru, konfigurovat nastavení parametrů antispamového jádra a dalších úrovní ochrany.



3.3.1 Microsoft Exchange Server

3.3.1.1 Transportní Agent

Zde můžete nastavit možnosti ochrany proti spamu pomocí transportního agenta.



POZNÁMKA: Transportní agent není ve verzi Microsoft Exchange Server 5.5.

Pokud zapnete možnost **Povolit antispamovou ochranu transportním agentem**, můžete nastavit jaká akce se má provést pro nevyžádané zprávy (SPAM) - **Provést akci na nevyžádaných zprávách:**

- **Ponechat zprávu** - zachovat zprávu i přesto, že byla označena jako SPAM
- **Poslat zprávu do karantény** - přesunout zprávu označenou jako SPAM do karantény zpráv
- **Vymazat zprávu** - vymazat zprávu označenou jako nevyžádaná

Pokud chcete, aby záhlaví zprávy obsahovala výši zjištěného spamové skóre, zapněte možnost **Zapisovat SPAM skóre do kontrolovaných zpráv**.

Aktivováním možnosti **Povolit techniku Greylisting** zapnete funkcionalitu, která chrání uživatele pro spamem tímto způsobem: Transportní agent pošle obratem SMTP hodnotu "Temporarily rejected", tj. "dočasně zamítnuta" (přednastavená je 451/4.7.1) na každou přijatou zprávu, která nepochází z identifikovaného zdroje. Legitimní server se pokusí zprávu po určitém zdržení znovu přeposlat. Servery odesílající spam se obvykle nepokoušejí tyto zprávy při neúspěšném doručení znovu odeslat, protože odesílají tísíce emailových adres najednou a nemají čas na zpětnou kontrolu. Greylisting je další účinnou vrstvou ochrany před spamem a nemá žádný vliv na hodnotící schopnosti antispamového modulu.

Při vyhodnocování zdroje zprávy se berou v úvahu nastavení na seznamech: **Povolené IP adresy, Ignorované IP adresy**, seznamy **Safe Senders** a **Allow IP** definované na Exchange Serveru, a také nastavení AntispamBypass pro daný mailbox. Zprávy z těchto IP adres / Safe Sender seznamů, resp. zprávy doručovány do schránky se zapnutým AntispamBypass budou z kontroly pomocí metody Greylisting vynechány.

V poli **SMTP odpověď pro dočasně odmítnuté spojení:** lze nastavit dočasnou odpověď poslána SMTP serveru.

Příklad SMTP odpovědi:

Primární kód odpovědi	Doplňkový kód stavu	Popis

451	4.7.1	Requested action aborted: local error in processing

UPOZORNĚNÍ: Použití nesprávné syntaxe v kódech odpovědí SMTP, může vést k chybám v ochraně pomocí greylisting, následkem kterých může dojít k doručení potenciálních spamových zpráv nebo nedoručení legitimních zpráv apod.

Časový limit pro počáteční zamítnutí spojení (v minutách) - pokud je zpráva doručena poprvé a dočasně zamítnuta, toto nastavení vymezuje časový úsek, během kterého bude tato zpráva odmítaná (měřeno od prvního zamítnutí). Po uplynutí nastaveného času bude zpráva úspěšně přijata. Nejmenší hodnota, kterou sem můžete zadat je 1 minuta.

Čas expirace neověřených spojení (v hodinách) - toto nastavení určuje minimální časový interval, během kterého zůstanou uloženy údaje triplety. Legitimní server musí přeposlat požadovanou zprávu před ukončením této periody. Tato hodnota musí být větší než hodnota **Časový limit pro počáteční zamítnutí spojení**.

Čas expirace ověřených spojení (ve dnech) - nejmenší počet dní, během nichž bude uložena informace o triplety a během kterých lze přijímat zprávy od určitého odesílatele bez jakéhokoli zdržení. Tato hodnota musí být větší než hodnota **Čas expirace neověřených spojení (v hodnotách).**

POZNÁMKA: Při sestavování SMTP odpovědi můžete použít i systémové proměnné.

3.3.2 Antispamové jadro

Zde máte možnost nastavit parametry **Antispamového jádra**. Stisknutím tlačítka **Nastavit...**, se otevře okno s parametry antispamového jádra 37, které jdou konfigurovat.

Kategorizace zpráv

Antispamové jádro ESET Mail Security přiřazuje každé oskenování zprávě skóre od 0 do 100. Nastavení limitů spam skóre v této sekci mají vliv:

1) na to, zda zpráva bude vyhodnocena jako SPAM, nebo jako ne SPAM. Všechny zprávy se stejným nebo vyšším skóre než je hodnota **Hodnota skóre, od které je zpráva považována určitě za SPAM:** budou považovány za SPAM. Na těchto zprávach se vykonají akce podle nastavení Transportního agenta 35.

2) na to, zda se zpráva zaznamená do antispam protokolu 79 (**Nástroje** > **Protokoly** > **Antispam**). Do protokolu se zaznamenávají zprávy, které mají hodnotu spam skóre vyšší nebo shodnou s hodnotou **Hodnota skóre určující hranici, kdy je zpráva považována za pravděpodobný SPAM nebo pravděpodobně čistou:.**

3) na to, do které kategorie v rámci antispamové statistiky bude zpráva započítána (**Stav ochrany** > **Statistiky** > **Antispamová ochrana poštovních serverů**):

Zprávy vyhodnocené jako SPAM: – hodnoty stejné nebo větší než je hodnota **Hodnota skóre**, **od níž je zpráva považována určitě za SPAM.**

Zprávy vyhodnocené jako pravděpodobně SPAM: - hodnoty rovné nebo větší než je hodnota **Hodnota skóre určující hranici, kdy je zpráva považována za pravděpodobný SPAM nebo pravedpodobne čistou.**

Zprávy vyhodnocené jako pravděpodobně NE SPAM: - hodnoty menší než je hodnota **Hodnota skóre určující hranici, kdy je zpráva považována za pravděpodobný SPAM nebo pravedpodobne čistou.**

Zprávy vyhodnoceny jako určitě NE SPAM: - hodnoty rovné nebo menší než je hodnota **Hodnota skóre, do níž je zpráva považována určitě za čistou.**

3.3.2.1 Nastavení parametrů antispamového jádra

Nastavení parametrů antispamového jádra
Můžete si vybrat jeden z přednastavených profilů konfigurace (**Doporučená, Maximální přesnost, Maximální rychlost, Vlastní**). Seznam profilů se nahraje z antispamového modulu. Při všech konfiguracích se při startu antispamového modulu aplikují nastavení ze souboru *spamcatcher.conf*, s tím, že se vybraná podmnožina nastavení, specifických pro danou konfiguraci, aplikuje přímo z programu. Dokonce i při konfiguraci **Vlastní** se některá nastavení berou primárně z programu a nikoli ze souboru spamcatcher.conf - např. nastavení týkající se proxy serveru zadané v *spamcatcher.conf* se nepoužijí, pokud jsou zároveň zadáno přímo přes grafické rozhraní ESET Mail Security, neboť ty mají přednost. Dále, vždy se přepíše nastavení možnosti automatické aktualizace antispamového jádra - je to vypnuto vždy, bez ohledu na to, co zadá uživatel do *spamcatcher.conf*.

Detaily naleznete v kapitole Konfigurační soubor 39.

Nastavení **Doporučená** v sobě spojuje doporučené nastavení v rovnovážném vztahu mezi úrovní bezpečnosti a zátěží kladenou na systém.
Nastavení **Maximální přesnost** se zaměřuje výhradně na bezpečnost poštovního serveru. Toto nastavení spotřebuje více systémových zdrojů než Doporučená konfigurace.
Nastavení **Maximální rychlost** optimalizuje parametry (i vypínáním některých funkcionalit kontroly) modulu tak, aby byla spotřeba systémových zdrojů co nejnižší.
Nastavení **Vlastní> Otevřít konfigurační soubor** umožní uživateli upravit soubor *spamcatcher.conf*. Požití této možnosti doporučujeme pouze pro systémovým administrátorům, který si přejí upravit systém do nejmenšího detailu (pokud je to nutné). Přestože první tři možnosti by měly pokrývat většinu potřeb nastavení. Pokud chcete použít Vlastní konfiguraci, přečtěte si kapitolu Konfigurační soubor 39, kde jsou detaily o jednotlivých dostupných parametrů, a jaký mají tyto parametry efekt na systém. Prosím, vezměte na vědomí, že je stále několik nastavení, které jsou aplikovány přímo z programu a tím pádem mají prioritu nad nastavením z konfiguračního souboru *spamcatcher.conf*. Toto je zabezpečení nejdůležitějších komponent proti nesprávným nastavením, které by jinak měly za následek nesprávné fungování programu ESET Mail Security.

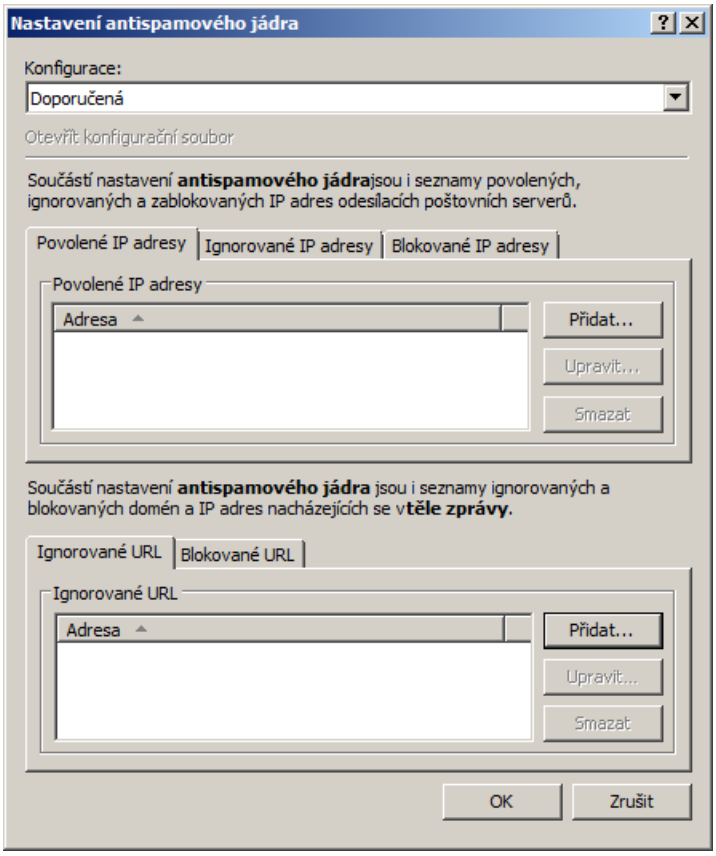
Jsou dva způsoby jak změnit nastavení v souboru *spamcatcher.conf*. Jako první možnost můžete použít grafické rozhraní (GUI) programu ESET Mail Security zvolením **Vlastní** v rozbalovacím menu **Konfigurace**: a následným kliknutím na linku **Otevřít konfigurační soubor**. Tímto se otevře soubor *spamcatcher.conf* na editaci v aplikaci Poznámkový blok (Notepad). Druhá možnost je otevřít soubor *spamcatcher.conf* přímo v jakémkoli jiném textovém editoru. *Soubor spamcatcher.conf* najdete v složce *C: \ Documents and Settings \ All Users \ Application Data \ ESET \ ESET Mail Security \ MailServer* (platí pro Windows Server 2000 and 2003) a ve složce *C: \ programdata \ ESET \ ESET Mail Security \ MailServer (platí pro Windows Server 2008).*

Po modifikaci souboru *spamcatcher.conf* se požadovanými parametry je třeba restartovat antispamové jádro na to, aby systém mohl použít nové změny konfigurace programu a nové parametry ze souboru *spamcatcher.conf*. V případě, že jste editovali spamcatcher.conf přes GUI, můžete jednoduše zavřít okno kliknutím na tlačítko OK. Tímto se antispamové jádro samy restartuje. Můžete si všimnout, že linka **Opětovné načtení nastavení antispamového jádra** zůstane vyšednutá, což znamená, že antispamové jádro se restartuje.

V případě, že jste konfigurační soubor *spamcatcher.conf* modifikovali pomocí textového editoru přímo (bez použití GUI), pak je nutné restartovat antispamové jádro na to, aby program použil nové nastavení. Je několik způsobů jak se asntipamové jádro dá restartovat. Můžete nechat antispamové jádro aby restartovali při nejbližší události (např. při aktualizaci virové databáze), nebo, pokud je to nezbytné a nechcete čekat, můžete restartovat jádro ihned otevřením stromu pokročilých nastavení (**F5**), nabídka **Ochrana serveru> Antispamová ochrana> Antispamové jádro** a kliknutím na linku **Opětovné načtení nastavení antispamového jádra**. Případně můžete restartovat antispamové jádro pomocí vypnutí a opětovného zapnutí antispamové ochrany z hlavního menu programu ESET Mail Security navigování do **Nastavení> Antispamová ochrana** a kliknutím na **Dočasně vypnout antispamovou ochranu** ve spodní části okna, a následně kliknutím na **Zapnout antispamovou ochranu.**

Po těchto krocích začne antispamové jádro používat novou konfiguraci.

POZNÁMKA: Máte možnost použít editovaný soubor *spamcatcher.conf* s vašimi vlastními nastaveními a zároveň používat jinou konfiguraci než **Vlastní** (např. **Maximální přesnost**). V takovém případě budou použity některé nastavení ze souboru *spamcatcher.conf* a některé vámi definované v GUI. Pro ty nastavení, které jsou rozdílné platí, že nastavení z GUI mají vždy prioritu nad těmi ze souboru *spamcatcher.conf* (s výjimkou nastavení nejdůležitějších komponent - které jsou definovány programem bez ohledu na to, co je nastaveno přes GUI nebo ze souboru *spamcatcher.conf*)



V záložce **Povolené IP adresy** můžete přidávat IP adresy, které mají mít statut povoleno, tj. když první neignorovaná IP adresou v Přijatých hlavičkách souhlasí s kteroukoliv adresou v tomto seznamu, zpráva přidělí skóre 0 a více se již nekontroluje.

V záložce **Ignorované IP adresy** můžete přidat IP adresy, které budou ignorovány při RBL (Real-time Blackhole List) kontrolách. Tady by se měly nacházet všechny IP adresy firewallu, které nejsou přímo dostupné z Internetu. Přidáním takových adres zabráníte zbytečným kontrolám a umožníte systému identifikovat opravdu se připojující IP adresy. Interní IP adresy jsou opomíjeny programem automaticky (192.168.xy a 10.x).

V záložce **Blokované IP adresy** můžete přidávat IP adresy, které by měly být blokovány, tj. jestliže jakákoli neignorovaná IP adresa v Přijatých záhlavích souhlasí s kteroukoliv adresou v tomto seznamu, zprávě se přidělí skóre 100 a již neprobíhají žádné ostatní kontroly.

V záložce **Ignorované domény** můžete přidávat domény použité v tělech zpráv, které mají být vždy vyloučeny z kontrol DNSBL a MSBL a ignorovány.

V záložce **Blokováno domény** můžete přidávat domény použité v tělech zpráv, které mají být vždy blokovány.

POZNÁMKA: Na rozdíl od konfigurace IP adres se při přidávání domén nedají použít zástupné znaky (tzv. wildcards).

Technologie antispamu i Greylisting umožňuje použít metodu tzv. whitelisting.

Možnosti použití whitelisting pro greylisting

Microsoft Exchange 2003
- seznam povolených IP adres v Exchange IMF (**Connection filtering > Global Accept List**)
- seznam povolených a ignorovaných IP adres v nastavení ESET Mail Security

Microsoft Exchange 2007/2010
- seznam povolených a ignorovaných IP adres v nastavení ESET Mail Security
- seznam Safe-senders pro daného příjemce
- příznak AntispamBypassEnabled na daném mailboxu
- seznam povolených IP adres v Microsoft Exchange

- příznak AntispamBypass pro dané SMTP spojení

Možnosti použití whitelistingu pro antispam

Všeobecné
- seznam povolených IP adres v nastavení ESET Mail Security
- seznam mailových domén v souboru *approvedsenders*
- filtrování na základě pravidel

Microsoft Exchange 2003
- seznam povolených IP adres v Exchange IMF (**Connection filtering > Global Accept List**)

Microsoft Exchange 2007/2010
- seznam Safe-senders pro daného příjemce
- příznak AntispamBypassEnabled na daném mailboxu
- seznam povolených IP adres v Microsoft Exchange
- příznak AntispamBypass pro dané SMTP spojení

POZNÁMKA: Společné pro technologii antispamu a Greylisting je, že zprávy z totožností a interních zdrojů se na spam nekontrolují.

3.3.2.1.1 Konfigurační soubor

Konfigurační soubor *spamcatcher.conf* obsahuje řadu dalších nastavení, které nejsou dostupné přes grafické rozhraní (GUI) ESET Mail Security, ovšem lze je měnit právě prostřednictvím tohoto souboru. Nastavení v *spamcatcher.conf* jsou přehledně strukturovány a mají svoji formu. Každé z nastavení obsahuje tyto položky:

Name - název nastavení
Arguments - hodnoty, které může nastavení získat a formát v jakém se zapisují
Default - Standardní hodnota nastavení
Description - podrobný opis/vysvětlení k nastavení

Prázdné řádky, stejně jako řádky začínající znakem # jsou ignorovány.

Seznam nejdůležitějších nastavení souboru *spamcatcher.conf*:

Název nastavení	Detaily
approved_ip_list	Seznam povolených IP adres. Není nutné jej zadávat do *spamcatcher.conf*, nastavuje se přímo přes grafické rozhraní programu (viz kapitola Nastavení parametrů antispamového jádra 37).
blocked_ip_list	Seznam blokovaných IP adres. Není nutné jej zadávat do *spamcatcher.conf*, nastavuje se přímo přes grafické rozhraní programu (viz kapitola Nastavení parametrů antispamového jádra 37).
ignored_ip_list	Seznam ignorovaných IP adres. Není nutné jej zadávat do *spamcatcher.conf*, nastavuje se přímo přes grafické rozhraní programu (viz kapitola Nastavení parametrů antispamového jádra 37).
rbl_list	Seznam Realtime Blackhole serverů, které mají být použity při vyhodnocování zprávy. RBL požadavek spočívá v kontrole, zda se konkrétní IP adresa nachází na daném RBL serveru. Kontrolované jsou IP adresy nacházející se v sekcích Received: v hlavičce emailu. Formát zápisu je: `rbl_list=server:response:offset,server2:response2:offset2,...` Význam jednotlivých parametrů: 1) server - jméno RBL serveru 2) response - odpověď RBL serveru v případě pokud se na něm daná IP adresa nachází (standardní odpovědi jsou 127.0.0.2, 127.0.0.3, 127.0.0.4. atd..). Je to nepovinný parametr a pokud není definován, v úvahu se berou všechny odpovědi. 3) offset - hodnota od 0 do 100. Ovlivňuje celkové spam skóre zprávy. Standardní hodnota je 100, což znamená, že v případě pozitivního nálezu je zprávě přiděleno spam skóre 100 a je tak vyhodnocena jako spam. Záporné hodnoty ubírají z celkového spam skóre zprávy. Hodnotu 0

	očekávejte také v případech, že jde o zprávy od odesilatelů ze souboru *approvedsenders* a hodnotu 100 zase pokud se jedná o zprávy odesílatelů ze souboru blockedsenders (viz níže).
	
	Příklad 1:
	`rbl_list=ent.adbl.org`
	RBL kontrola probíhá vůči serveru `ent.adbl.org` a v případě pozitívního nálezu je zprávě přiřazen standardní offset 100, čím je zpráva jednoznačne označena jako spam.
	
	Příklad 2:
	`rbl_list=ent.adbl.org::60`
	RBL kontrola probíhá vůči serveru `ent.adbl.org` a v případě pozitívního nálezu je zprávě přiřazen offset 60, což zvyšuje celkové spam skóre zprávy
	
	Příklad 3:
	`rbl_list=bx9.dbl.com::85, list.dnb.org:127.0.0.4:35, req.gsender.org::-75`
	RBL kontrola probíhá vůči definovaným serverům (zleva doprava). V případě pozitivního nálezu na `bx9.dbl.com` je použit offset 85. V případě pozitivního nálezu na `list.dnb.org` a odpovědi 127.0.0.4 je použit offset 35. V případě jiné odpovědi než 127.0.0.4 není offset aplikován. V případě pozitivního nálezu na `req.gsender.org` se spam skóre sníží o 75 bodů (záporná hodnota).

rbl_max_ips	Maximální počet IP adres, které se posílají na kontrolu RBL serveru. Celkový počet RBL požadavků přitom skládá z počtu IP adres nacházejících se v sekcích Received: v hlavičce emailu (až do limitu definovaného v rbl_maxcheck_ips) násobeno počtem RBL serverů definovaném v rbl_list. Hodnota 0 znamená kontrolu neomezeného počtu IP adres. IP adresy nacházející se v ignored_ip_list (tj. v seznamu **Ignorované IP adresy** v nastaveních ESET Mail Security) se do limitu rbl_max_ips nezapočítávají. Toto nastavení se aplikuje pouze pokud je rbl_list aktivován (obsahuje alespoň jeden server).
approved_domain_list	Jde o seznam domén a IP adres nacházejících se v těle emailu, které mají být povoleny. Nepoužívat na whitelistovanie mailů podle domény odesílatele!
blocked_domain_list	Seznam domén a IP adres nacházejících se v těle emailu, které mají být vždy blokovány. Nejde o blacklist na adresu odesilatele! Není nutné jej zadávat do *spamcatcher.conf*, nastavuje se přímo přes grafické rozhraní programu (viz kapitola Nastavení parametrů antispamového jádra 37).
ignored_domain_list	Seznam domén nacházejících se v těle emailu, které mají být vždy vyloučeny z DNSBL kontroly a ignorovány. Není nutné jej zadávat do *spamcatcher.conf*, nastavuje se přímo přes grafické rozhraní programu (viz kapitola Nastavení parametrů antispamového jádra 37).

dnsbl_list	Seznam DNSBL serverů vůči nimž se mají kontrolovat domény a IP adresy nacházející se v těle emailu. Formát zápisu je
	
	`dnsbl_list=server:response:offset,server2:response2:offset2,...`
	
	Význam jednotlivých parametrů:
	1) server - jméno DNSBL serveru
	2) response - odpověď DNSBL serveru v případě pokud se na něm daná IP adresa / doména nachází (standardní odpovědi jsou 127.0.0.2, 127.0.0.3, 127.0.0.4. atd..). Je to nepovinný parametr a pokud není definován, v úvahu se berou všechny odpovědi.
	3) offset - hodnota od 0 do 100. Ovlivňuje celkové spam skóre zprávy. Standardní hodnota je 100, což znamená, že v případě pozitivního nálezu je zprávě přiděleno spam skóre 100 a je tak vyhodnocena jako spam. Záporné hodnoty ubírají z celkového spam skóre zprávy. Hodnotu 0 očekávejte také v případech, že jde o zprávy od odesilatelů ze souboru *approvedsenders* a hodnotu 100 zase pokud se jedná o zprávy odesílatelů ze souboru blockedsenders (viz níže).
	
	Kontrola prostřednictvím DNSBL může výrazně negativně ovlivnit výkon, protože každá doména / IP adresa z těla zprávy je kontrolována vůči všem definovaným DNSBL serverem a každá taková kontrola vyžaduje požadavek vůči DNS serveru. Ztrátu výkonu lze zmírnit nasazením DNS cache serveru pro tento účel. Z důvodu výkonu jsou z kontroly vynechány non-routable IP adresy (10.xxx, 127.xxx, 192.168.xx).
	
	Příklad 1:
	`dnsbl_list=ent.adbl.org`
	DNSBL kontrola probíhá vůči serveru `ent.adbl.org` a v případě pozitivního nálezu je zprávě

	přiřazen standardní offset 100, čím je zpráva jednoznačně označena jako spam.
	
	Příklad 2:
	`dnsbl_list=ent.adbl.org::60`
	DNSBL kontrola probíhá vůči serveru `ent.adbl.org` a v případě pozitivního nálezu je zpráve přiřazen offset 60, což zvyšuje celkové spam skóre zprávy
	
	Příklad 3:
	`dnsbl_list=bx9.dbl.com::85, list.dnb.org:127.0.0.4:35, req.gsender.org::-75`
	DNSBL kontrola probíhá vůči definovaným serverům (zleva doprava). V případě pozitivního nálezu na `bx9.dbl.com` je použit offset 85. V případě pozitivního nálezu na `list.dnb.org` a odpovědi `127.0.0.4` je použit offset 35. V případě jiné odpovědi než 127.0.0.4 není offset aplikován. V případě pozitivního nálezu na `req.gsender.org` se spam skóre sníží o 75 bodů (záporná hodnota).

home_country_list	Seznam zemí, které budou považovány za "domácí". Zprávy směrovány přes zemi, která není v tomto seznamu bude přísnější hodnocena (přidáním vyššího spam skóre). Země se do seznamu zadávají jako dvoupísmenný kód podle normy ISO 3166.
home_language_list	Seznam preferovaných jazyků - tj. nejpoužívanějších jazyků ve vašich emailových zprávách. Takové zprávy jsou z pohledu spam skóre méně přísné hodnocené. Jazyky se do seznamu zadávají jako dvoupísmenný kód podle normy ISO 639.
custom_rules_list	Umožňuje definovat vlastní seznamy pravidel, přičemž tyto jsou uloženy ve zvláštním souboru / souborech. Pravidla se v souboru nacházejí každé na samostatném řádku a mají tento formát: **Phrase**, **Type**, **Confidence**, **CaseSensitivity** **Phrase** - může to být jakýkoli text neobsahující čárku (,) **Type** - může mít tyto hodnoty: SPAM, Phish, BOUNCE, ADULT, FRAUDE. Pokud zadáte jakoukoli jinou hodnotu, automaticky bude použita hodnota SPAM. Typ SPAM představuje fráze vyskytující se v klasických spamových zprávách (nabízení různých výrobků). Typ Phish představuje fráze vyskytující se v podvodných zprávách (phishing), jejichž cílem je získat od uživatele citlivé údaje (jména, hesla, číslo kreditní karty apod.). Typ BOUNCE představuje fráze používané v automatických zprávách ze serverů - Non-Delivery Notification (typické při spoofovaní adresy odesilatele). Typ ADULT představuje fráze typické pro zprávy s pornografickým obsahem. Typ FRAUDE představuje fráze vyskytující se v podvodných emailech (tzv. Scam) nabízejících často různé podezřelé bankovní operace (převody peněz přes Vaše konto apod.). Typickým představitelem tohoto typu spamu je tzv.. Nigerijský spam. **Confidence** - hodnota od 0 do 100. Vůči Type určuje pravděpodobnost s jakou fráze patří do dané kategorie. Pokud je například Type Phish a Confidence 90, znamená to, že daná fráze se s velkou pravděpodobností vyskytuje ve zprávách typu phishing. Čím vyšší je hodnota Confidence, tím větší vliv má na celkové spam skóre zprávy. Hodnota 100 představuje speciální případ, kdy výsledné spam skóre zprávy bude také 100 a zpráva tak bude označena jako 100% spam. Podobně při hodnotě 0 bude zpráva označena jako ne spam. **CaseSensitivity** - hodnota 0 nebo 1. 0 znamená, že Phrase je case insensitive. 1 znamená, že Phrase je case sensitive. Příklady: replica, SPAM, 100, 0 Dear eBay member, PHISH, 90, 1 return to sender, BOUNCE, 80, 0

Další možnosti blacklistovania / whitelistovania představují soubory *approvedsenders a blockedsenders* (bez koncovky), které se spolu se souborem *spamcatcher.conf* nacházejí v adresáři *C: \ Documents and Settings \ All Users \ Application Data \ ESET \ ESET Mail Security \ MailServer* (pro Windows Server 2000 a 2003) av adresáři *C: \ programdata \ ESET \ ESET Mail Security \ MailServer* (pro Windows Server 2008). Je možné do nich přidat adresy odesílatelů, příp. pouze domény, přičemž soubor *approvedsenders* představuje seznam povolených adres / domén, zatímco soubor *blockedsenders* představuje seznam blokovaných adres / domén.

UPOZORNĚNÍ: Že adresa odesilatele bývá často padělání, použití souborů *approvedsenders a blockedsenders* není doporučený způsob whitelistovania / blacklistovania. Spolehlivější je používat seznamy povolených a blokovaných IP adres. Pokud z nějakého důvodu potřebujete použít whitelistovanie podle adresy / domény odesílatele (soubor

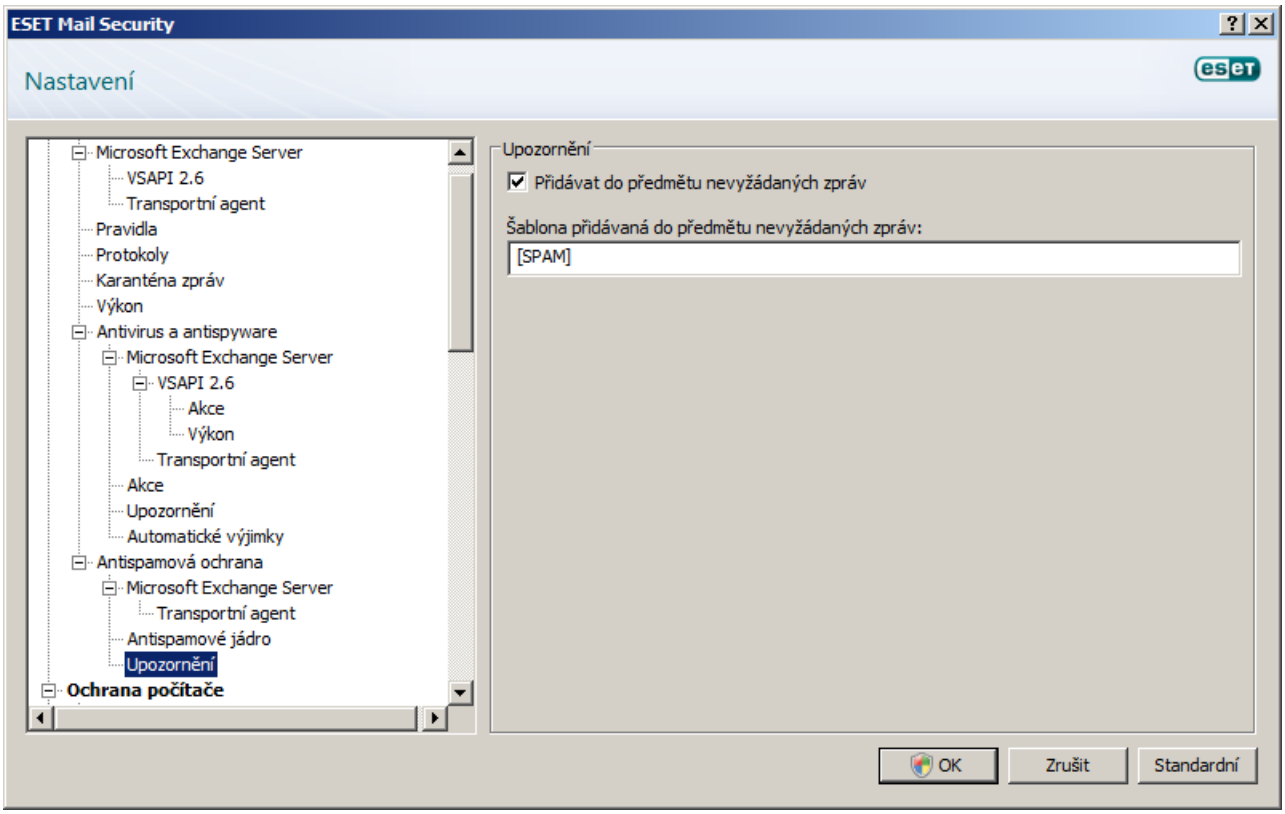
approvedsenders), měla by být vždy použita i některá další efektivní technologie kontroly (např. SPF).

Některé další nastavení:

enable_spf	Tato volba zapíná / vypíná kontrolu prostřednictvím Sender Policy Framework. Kontrola spočívá v ověření, zda je odesílatel oprávněn odesílat zprávy z dané domény - na základě zveřejněných pravidel dané domény (domain policy).
enable_all_spf	Tato volba rozhoduje o tom, zda domény, které nejsou v spf_list nebo v Mailshell souboru s pravidly, mohou obejít SPF kontrolu. Pro správné fungování musí být volba enable_realtime_spf nastavena na yes.
enable_realtime_spf	Pokud je tato volba zapnuta, při SPF kontrole se budou posílat DNS požadavky v reálném čase. Může to mít negativní dopad na výkon (zdržení při vyhodnocování zprávy).
spf_list	Tato volba umožňuje ovlivnit SPF záznam domény prostřednictvím přiřazení váhy danému SPF záznamu, čímž lze ovlivnit celkové spam skóre zprávy.
spf_*_weight	Hvězdička (Asterisk) uprostřed představuje 14 možných výsledků z SPF kontroly (viz *spamcatcher.conf* pro více detailů). Hodnota zadaná v tomto nastavení představuje tzv. vyvážení (offset), které se aplikuje na spam skóre pro jednotlivé typy výsledků. Pokud je například výsledek SPF kontroly "fail", tak se aplikuje vyvážení z nastavení spf_fail_weight. Od hodnoty vyvážení pak závisí, zda se celkové spam skóre zvýší nebo sníží.
spf_recursion_depth	Maximální hloubka vnoření (použití mechanismu "include"). Podle normy RFC 4408 je tento limit specifikovaný na 10 (kvůli zabránění Denial-of-Service), avšak některé současné SPF záznamy toto nesplňují a musí používat více úrovní vnoření aby byla SPF požadavek zcela vyhodnocena.
enable_livefeed_sender_repute	Pokud je tato volba vypnuta, SPF informace z LiveFeed bude ignorována.

3.3.3 Upozornění

Do předmětu každého e-mailu, který byl překontrolován pomocí ESET Mail Security a označen jako spam můžete přidat vlastní poznámku. Standardně se přidává poznámka ve tvaru [SPAM], případně si uživatel může nadefinovat vlastní text.



POZNÁMKA: Při sestavování textu, který se přidá do předmětu zprávy můžete použít i systémové proměnné.

3.4 Otázky a odpovědi

Otázka: Po instalaci EMSX s antispamem přestaly přicházet e-maily do poštovních schránek.
Odpověď: Pokud máte aktivován greylisting, jde o normální chování. V prvních hodinách provozu EMSX mohou e-maily přicházet až s několikahodinovým zpožděním. V případě problémů doporučujeme greylisting vypnout, případně vhodně nakonfigurovat.

Otázka: Skenuje VSAPI při kontrole příloh mailových zpráv pouze soubory v příloze nebo i těla zpráv?
Odpověď: Počínaje verzí Microsoft Exchange Server 2000 SP2 skenuje VSAPI i těla zpráv.

Otázka: Proč po vypnutí volby VSAPI i nadále probíhá testování zpráv?
Odpověď: Změna nastavení ve VSAPI probíhá asynchronně,t.j. po požadavku o změnu nastavení VSAPI systém čeká, dokud budou dané požadavky vyžádány serverem Microsoft Exchange. Tento cyklický proces probíhá v přibližně minutových intervalech. Totéž samozřejmě platí i pro ostatní nastavení VSAPI.

Otázka: Může VSAPI smazat i celou zprávu, pokud obsahuje infikovanou přílohu?
Odpověď: Ano, VSAPI dokáže smazat celou zprávu. Na to je však nejprve nutné v nastaveních VSAPI v části **Akce** zvolit možnost **Smazat celou zprávu**. Tato možnost je dostupná v systémech Microsoft Exchange Server 2003 a novějších. Starší verze Microsoft Exchange Server odstraňování celých zpráv nepodporují.

Otázka: Testuje VSAPI i odesílané zprávy?
Odpověď: Ano, VSAPI testuje i odesílané zprávy, pokud nemáte ve Vašem mailovém programu nastaveno odesílání zpráv na jiný SMTP server, než váš Microsoft Exchange Server. Tato funkcionalita je dostupná pro verze Microsoft Exchange Server 2000 Service Pack 3 a novější.

Otázka: Je možné přes VSAPI nastavit text, který se bude přidávat do každé otestované zprávy, podobně jako to dělá transportní agent?
Odpověď: Přidávání textu do otestovaných zpráv přes VSAPI není možné, protože Microsoft Exchange Server tuto možnost nepodporuje.

Otázka: Stává se mi, že si některé zprávy nedokážu přes Microsoft Outlook otevřít. Čím to je?
Odpověď: S největší pravděpodobností je v nastavení VSAPI v části **Akce** aktivována v roletovém menu **Vykonat akci při neléčené infiltraci** možnost **Zablokovat** nebo máte přidané pravidlo s nastavenou akcí **Zablokovat**. Obě z těchto voleb způsobí, že se infikovaná zpráva, nebo zpráva spadající do daného pravidla, označí a Microsoft Exchange Server k ní zablokuje přístup.

Otázka: Co přesně vyjadřuje v nastaveních VSAPI v části **Výkon** položka **Časový limit odezvy**?
Odpověď: V případě, že máte nainstalován Microsoft Exchange Server 2000 SP2 nebo vyšší, jedná se o maximální čas v sekundách potřebný k dokončení skenování pro jedno vlákno pomocí VSAPI. Pokud není skenování dokončeno v tomto časovém limitu, Microsoft Exchange Server odmítne klientovi přístup ke zprávě. Skenování přitom není přerušeno a po jeho dokončení bude každý další pokus klienta o přístup k této zprávě úspěšný. Pokud ale máte nainstalován Microsoft Exchange Server 5.5 SP3 nebo SP4, hodnota je udávána v milisekundách a vyjadřuje čas za jaký se má klient znovu pokoušet o přístup k souboru, který mu byl odmítnut z důvodu nevyřízené skenování.

Otázka: Jaký dlouhý může být seznam přípon souborů v jednom pravidle?
Odpověď: Seznam přípon souborů v jednom pravidle může být dlouhý až 255 znaků.

Otázka: Mám ve VSAPI nastavenu možnost **Testovat na pozadí**. Dosud se po každé aktualizaci virové databáze zprávy pro Microsoft Exchange Serveru vždy znovu zkontrolovaly. Po poslední aktualizací se tak ale nestalo. V čem je problém?
Odpověď: Microsoft Exchange Server si sám určuje, zda bude po aktualizaci virové databáze skenovat všechny zprávy okamžitě, nebo zda se kontrola provádí až při požadavku klienta o přístup k dané zprávě. Microsoft Exchange Server zkontroluje každou zprávu předtím, než ji doručí do klientské složky přijatých zpráv.

Otázka: Proč se při přijetí jedné zprávy může počítadlo pravidel zvýšit i o více než jedna?
Odpověď: Pravidla se porovnávají se zprávou při jejím zpracování transportním agentem (TA) nebo VSAPI. Pokud je povolena kontrola zpráv prostřednictvím TA i VSAPI, při příchodu zprávy se počítadlo pravidel může zvýšit i o 2 nebo více. VSAPI přistupuje k jednotlivým částem zprávy (tělo, příloha) zvlášť, a následně i pravidla se použijí pro každou část zvlášť. Navíc, pravidla se aplikují i při kontrole probíhající na pozadí (např. při opakovaném skenování úložiště poštovní schránky (mailbox) po každé aktualizaci virové databáze), což může rovněž přispět ke zvýšení stavu

počítadla.

Otázka: Je ESET Mail Security kompatibilní s Exchange Intelligent Message Filter (IMF)?
Odpověď: Ano, ESET Mail Security funguje s IMF. Způsob zpracování emailů vyhodnocených jako spam je v této konfigurací následující:

- Pokud má antispamový modul ESET Mail Security nastavenou akci **Smazat zprávu** (nebo **Přesunout zprávu do karantény**) a na Exchange IMF je nastavena libovolná akce, provede se akce, která je nastavena v ESET Mail Security.
- Pokud má Antispamový modul ESET Mail Security nastavenou akci na **Ponechat zprávu**, pak se provede akce nastavená na IMF (např., Delete, Reject, Archive ...). Pro správné fungování této funkcionality na IMF je třeba, aby volba **Zapisovat stupeň nevyžádané pošty (SCL) do záhlaví kontrolovaných zpráv podle hodnoty SPAM skóre** byla zapnuta (pod **Ochrana serveru**> **Microsoft Exchange Server** > **Transportní agent**).

Otázka: Jak docílím, aby Microsoft Outlook ukládal nevyžádanou poštu do uživatelem definovaného složky?
Odpověď: Při standardním nastavení ESET Mail Security ukládá Microsoft Outlook nevyžádanou poštu do **Junk E-mail** složky. Toto chování zajišťuje volba **Zapisovat SPAM skóre do kontrolovaných zpráv** (**F5** > **Ochrana serveru** > **Antispamová ochrana** > **Microsoft Exchange Server** > **Transportní agent**). Pokud potřebujeme ukládat nevyžádanou poštu do jiné složky, třeba udělat následující:

1) V ESET Mail Security:
   - deaktivovat volbu **Zapisovat SPAM skóre do záhlaví a kontrolovaných zpráv**,
   - nastavit akci **Ponechat zprávu** pro zprávy označené jako spam,
   - nastavit přidávaní textu do předmětu nevyžádaných zpráv, např. "[SPAM]" (**Ochrana serveru** > **Antispamová ochrana** > **Upozornění**).

2) V Microsoft Outlook:
   - nastavit pravidlo, které na základě specifického textu v předmětu zprávy ("[SPAM]") přesune tuto zprávu do uživatelem definovaného složky

Otázka: Ve statistikách antispamové ochrany je velké množství emailů v kategorii **Nezkontrolované**. Jaké emaily nejsou skenovány antispamovou ochranou?
Odpověď: Do kategorie **Nezkontrolované** se započítávají:
Všeobecné:

- všechny zprávy skenované v době, kdy byla vypnuta antispamová ochrana na některé úrovni (mailserver, transportní agent)

Microsoft Exchange Server 2003:

- zprávy přicházející z IP adresy, která se nachází v IMF na seznamu **Global Accept List**
- zprávy od ověřených odesílatelů

Microsoft Exchange Server 2007:

- všechny zprávy posílané uvnitř organizace (ty jsou skenovány pouze antivirovou ochranou)
- zprávy od ověřených odesílatelů
- zprávy od odesílatelů konfigurovaných pro bypass antispamu
- všechny zprávy posílané do mailboxu, který má v Microsoft Exchange Serveru nastaven atribut **AntispamBypass**
- všechny zprávy posílané od odesílatelů, kteří se nacházejí na seznamu **Safe Senders**

Poznámka: Do kategorie **Nezkontrolované** nespadají adresy definované ve whitelistu v nastaveních antispamového jádra. Patří sem zprávy, které vůbec nebyli zpracované antispamem.

Otázka: Uživatelé si stahují poštu do svých emailových klientů přes POP3 (mimo MS Exchange Serveru), ale samotné poštovní schránky (mailboxes) jsou na MS Exchange Serveru. Bude tyto emaily kontrolovat ESET Mail Security na přítomnost virů a SPAMu?
Odpověď: Při takovéto konfigurací bude ESET Mail Security kontrolovat emaily uložené na MS Exchange Serveru pouze na přítomnost virů (prostřednictvím VSAPI). Antispamová kontrola nebude možná, protože probíhá na úrovni SMTP serveru.

Otázka: Je možné ovlivnit od jaké výšky spam skóre bude zpráva vyhodnocena jako spam?
Odpověď: Ano tato hranice se dá nastavit v ESET Mail Security počínaje verzí 4.3 (viz. kapitola Nastavení parametrů antispamového jádra 37).

Otázka: Kontroluje ESET Mail Security zprávy antispamovou ochranou, pokud jsou stahovány přes POP3 Connector?

Odpověď: Zprávy stahované přes POP3 Connector jsou kontrolovány antispamovou ochranou pouze na SBS 2008.

4. ESET Mail Security - ochrana serveru

Vedle ochrany Microsoft Exchange Serveru, obsahuje ESET Mail Security všechny potřebné nástroje pro zajištění ochrany serveru jako klientského počítače (rezidentní štít, ochrana při přístupu na web, ochrana poštovního klienta a ochrana proti nevyžádaným zprávám).

4.1 Antivirus a antispyware

Zabezpečuje komplexní ochranu před nebezpečnými programy ohrožujícími systém. Zahrnuje kontrolu souborů, e-mailů a internetové komunikace. Pokud antivirová ochrana zjistí škodlivý kód, zablokuje jej a poté jej vyléčí, odstraní nebo přesune do karantény.

4.1.1 Rezidentní ochrana

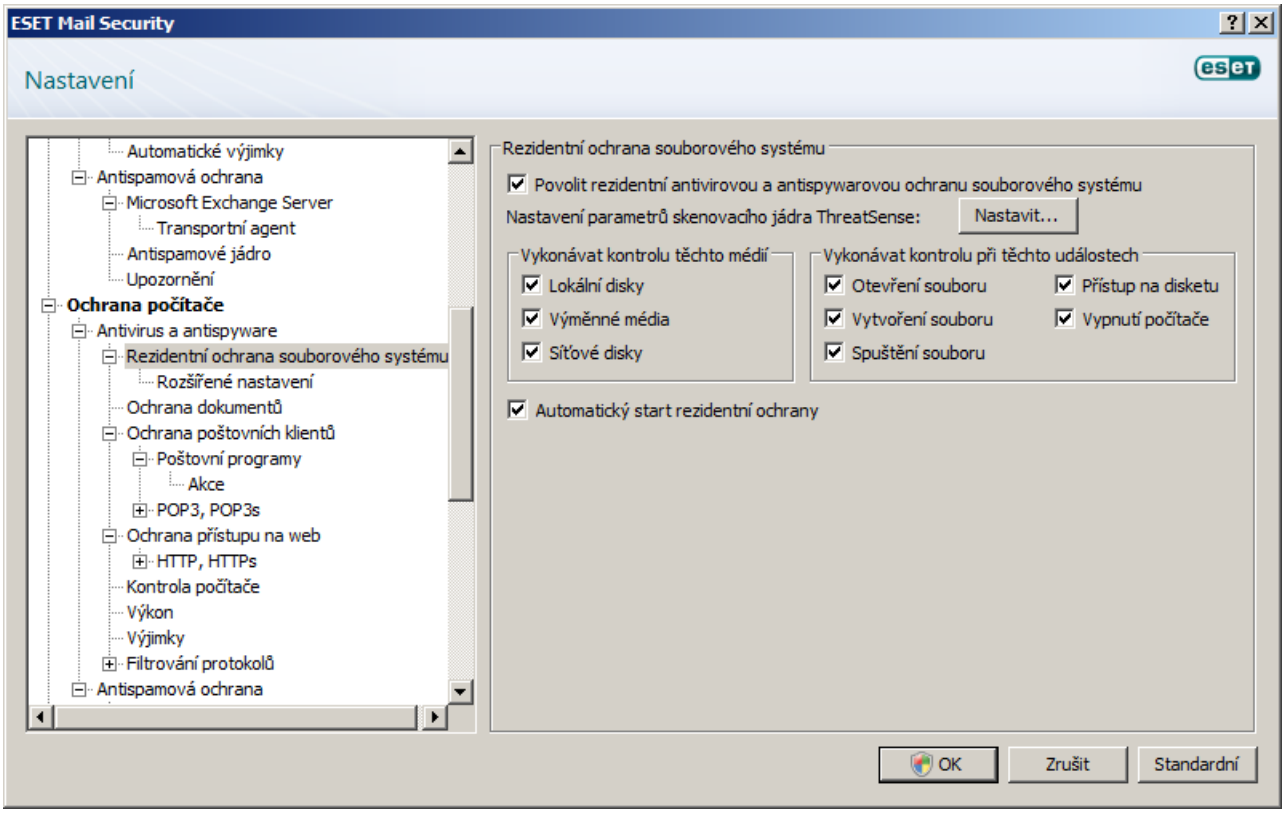
Kontroluje veškeré dění v počítači. Všechny soubory, které jsou v počítači otevírány, vytvářeny nebo spouštěny, jsou kontrolovány na přítomnost infiltrace. Rezidentní ochrana se spouští při spuštění operačního systému.

4.1.1.1 Nastavení kontroly

Rezidentní ochrana kontroluje různé typy médií a kontrola je prováděna při různých událostech. Při kontrole jsou používány detekční metody ThreatSense (ty jsou popsané v kapitole Nastavení skenovacího jádra ThreatSense 60). Chování kontroly může být jiné u nově vytvořených a u již existujících souborů. U nově vytvořených souborů lze nastavit hlubší úroveň kontroly.

Pro zajištění minimálního zatížení systému rezidentní ochranou, nejsou kontrolovány soubory, které již prošly kontrolou a nezměnily se. Soubory jsou opětovně zkontrolovány po aktualizaci virové databáze. Této vlastnosti odpovídá nastavení **Zapnout Smart optimalizaci**. Po vypnutí budou kontrolovány všechny soubory, ke kterým se přistupuje. Toto nastavení se dá změnit v **Pokročilých nastaveních** (klávesa **F5** kdekoli v hlavním menu programu) > **Ochrana počítače** > **Antivirus a antispyware** > **Rezidentní ochrana souborového systému** po stisknutí tlačítka **Nastavit...** > **Ostatní**.

Rezidentní ochrana se standardně spouští při startu operačního systému a zajišťuje nepřetržitou kontrolu počítače. Ve speciálních případech (například při konfliktu s jinou rezidentní ochranou) může být start rezidentní ochrany vypnut volbou **Automatický start rezidentní ochrany.**



4.1.1.1.1 Kontrola médií

Standardně je nastavena kontrola všech typů médií:

Lokální disky – lokální pevné disky v počítači

Výměnné média – diskety, USB flash disky, paměťové karty, atd.

Síťové disky – namapované disky

Doporučujeme zachovat kontrolu všech médií. Nastavení je doporučeno měnit pouze ve zvláštních případech, například pokud při kontrole určitého média dochází k výraznému zpomalení přenosu dat.

4.1.1.1.2 Kontrola při událostech

Standardně jsou soubory kontrolovány při otevírání, spouštění a vytváření a tato nastavení doporučujeme ponechat. Těmito nastaveními je zabezpečena kontrola veškerého dění v počítači.

Nastavení kontroly při **přístupu na disketu** a **vypnutí počítače** zabezpečují kontrolu boot sektoru diskety při přístupu na toto médium a boot sektorů pevného disku při vypínání počítače. I když v současné době jsou boot viry již téměř přežitkem, doporučujeme nastavení ponechat aktivní, protože se stále může objevit médium, které je boot virem infikováno.

4.1.1.1.3 Rozšířené nastavení

Podrobnější nastavení jsou přístupná v pokročilých nastaveních (F5) pod **Ochrana počítače** > **Antivirus a antispyware** > **Rezidentní ochrana souborového systému** > **Rozšířené nastavení**.

Doplňující parametry ThreatSense pro nověvytvořené a modifikované soubory - U nově vytvořených souborů je největší pravděpodobnost obsahu infiltrace. Z tohoto důvodu je pro tyto soubory zvýšená úroveň hloubky kontroly oproti kontrole již existujících souborů. Při kontrole se používá rozšířená heuristika, která má vysokou účinnost při detekci nových infiltrací. Kontrolovány jsou i samorozbalovací (SFX) archivy a runtime archivy (vnitřně komprimované spustitelné soubory). Archivy se standardně kontrolují do desáté úrovně vnoření a kontrolují se všechny, bez ohledu na jejich velikost (tomuto odpovídá volba **Standardní nastavení archivů**). Deaktivací této volby je možné tyto parametry měnit.

Doplňující parametry ThreatSense pro spuštěné soubory - Při spuštění souboru se standardně nepoužívá rozšířená heuristika, lze ji však v odůvodněných případech aktivovat volbou **Rozšířená heuristika při spuštění souboru**. Třeba mít na paměti, že za určitých okolností může aktivování této volby způsobit zpomalení spouštění

programů a chod celého počítače.

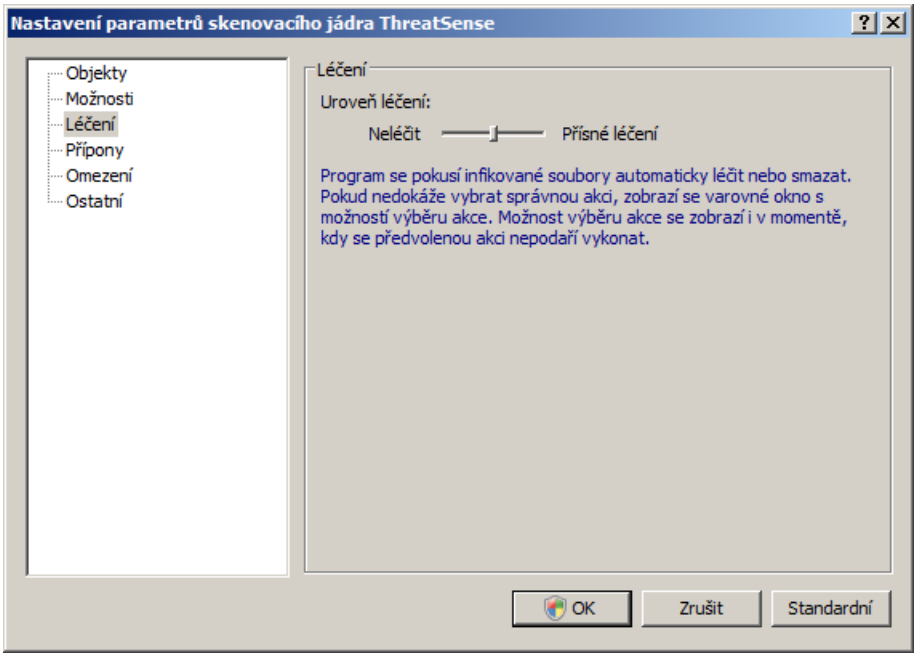
4.1.1.2 Úrovně léčení

Rezidentní ochrana pracuje ve třech režimech léčení:(nastavení možností **Léčení** je přístupné v položce **Rezidentní ochrana souborového systému** po kliknutí na tlačítko **Nastavit...**).

- V první úrovni **Neléčit** je uživateli při každé infiltraci zobrazeno varovné okno s možností výběru akce. Uživatel tak musí pro detekci infiltrace zvolit požadovanou akci. Tato úroveň je určena spíše pro pokročilé uživatele, kteří vědí, jakou akci mají zvolit při různých typech infiltrace.

- Střední úroveň automaticky zvolí akci, která se má provést s infikovaným souborem. O detekci a odstranění infikovaného objektu se zobrazí informační zpráva v pravém dolním rohu obrazovky. Automatická akce není provedena u archivů, které kromě infikovaného souboru obsahují i jiné soubory, a u souborů, u nichž aplikace není schopna vyhodnotit automatický postup.

- Třetí úroveň **Přísné léčení** je „nejagresivnější": odstraněny jsou všechny infikované objekty. U této úrovně existuje riziko ztráty bezproblémových dat. Tuto úroveň doporučujeme používat pouze ve zvláštních případech.



4.1.1.3 Kdy měnit nastavení rezidentní ochrany

Rezidentní ochrana je klíčovým modulem zabezpečujícím ochranu počítače. Proto je při změnách nastavení nezbytná opatrnost. Rezidentní ochranu doporučujeme měnit pouze ve specifických případech, například při konfliktu s určitou aplikací nebo rezidentní ochranou jiného antivirového programu.

Po instalaci aplikace ESET Mail Security jsou nastavení přednastavena tak, aby uživateli zajišťovala maximální bezpečnost systému. Standardní nastavení lze obnovit pomocí tlačítka **Standardní**, které se nachází v okně nastavení rezidentní ochrany.

4.1.1.4 Kontrola rezidentní ochrany

To, zda je rezidentní ochrana funkční a detekuje viry, je možné otestovat pomocí testovacího souboru eicar.com. Jedná se o soubor, který je detekován antivirovými programy. Soubor byl vytvořen společností EICAR (European Institute for Computer Antivirus Research) k testování funkčnosti antivirových programů. Soubor eicar.com je k dispozici ke stažení na adrese http://www.eicar.org/download/eicar.com

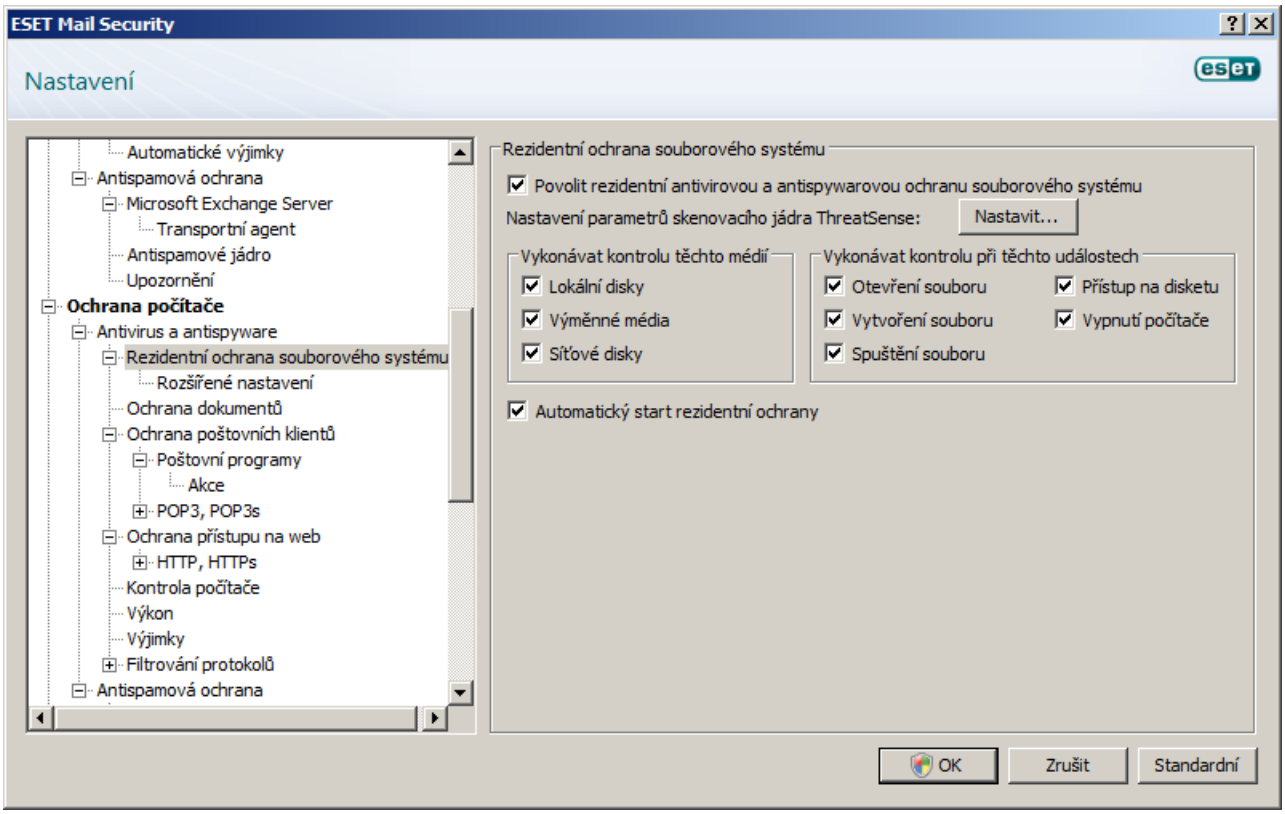
POZNÁMKA: Před kontrolou rezidentní ochrany je nutné vypnout firewall. V případě, že je firewall zapnut, testovací soubory budou rozpoznány a firewall neumožní jejich stažení.

4.1.1.5 Co dělat, když nefunguje rezidentní ochrana

V následující kapitole si popíšeme problémové stavy, které mohou nastat s rezidentní ochranou, a jak při nich postupovat.

Rezidentní ochrana je vypnuta
Prvním důvodem vypnutí rezidentní ochrany je vypnutí uživatelem. Opětovné zapnutí je možné v nastaveních rezidentní ochrany, kde je možné klepnout na příslušné tlačítko.

Pokud se rezidentní ochrana nespouští při startu operačního systému, je pravděpodobně vypnuta možnost **Automatický start rezidentní ochrany**. Tuto možnost lze zapnout v Rozšířených nastaveních ve větvi **Rezidentní ochrana souborového systému**, kde ji naleznete v části Rozšířené nastavení.



Rezidentní ochrana nedetekuje a neléčí infiltrace.
Přesvědčte se, zda nemáte nainstalován antivirový program jiné společnosti. Mezi dvěma rezidentními ochranami může docházet ke konfliktu, a proto je třeba jiný antivirový program odinstalovat.

Rezidentní ochrana se nespouští.
Pokud se rezidentní ochrana nespouští při startu systému ani při nastavení možnosti **Automatický start rezidentní ochrany**, dochází zřejmě ke konfliktu s jiným programem. V takovém případě doporučujeme kontaktovat technickou podporu společnosti ESET.

4.1.2 Ochrana poštovních klientů

Zabezpečuje kontrolu poštovní komunikace přijímané prostřednictvím protokolu POP3. Pomocí zásuvného programu (plug-in) pro klienta Microsoft Outlook je zabezpečena kontrola veškeré komunikace příslušného klienta (POP3, MAPI, IMAP, HTTP).

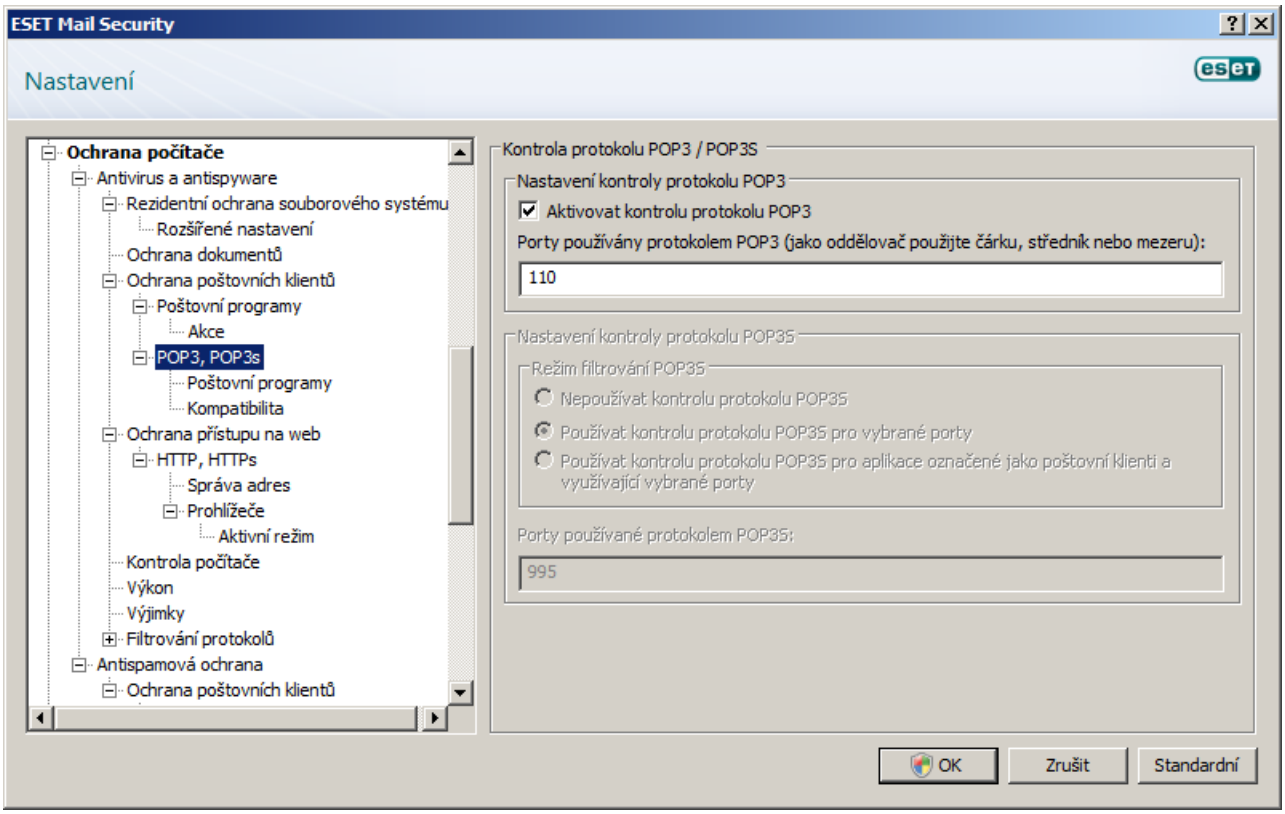
Při kontrole přijímaných zpráv jsou použity všechny pokročilé metody kontroly obsažené ve skenovacím jádře ThreatSense. Tím je zabezpečena detekce nebezpečných programů ještě před aktualizací detekčních databází. Kontrola POP3 protokolu je nezávislá na typu poštovního klienta.

4.1.2.1 Kontrola POP3 protokolu

Protokol POP3 je nejrozšířenější protokol, který slouží k přijímání e-mailové komunikace prostřednictvím poštovního klienta. Aplikace ESET Mail Security zabezpečuje ochranu tohoto protokolu bez ohledu na používaného klienta.

Modul zabezpečující kontrolu se zavádí při spuštění operačního systému a po celou dobu je zaveden v paměti. Pro správné fungování stačí zkontrolovat, zde je modul zapnut, a kontrola protokolu POP3 je prováděna automaticky bez nutnosti konfigurace poštovního klienta. Standardně je kontrolována komunikace na portu 110, v případě komunikace lze přidat používaný port. Čísla portů se oddělují čárkou.

Není kontrolována šifrovaná komunikace.



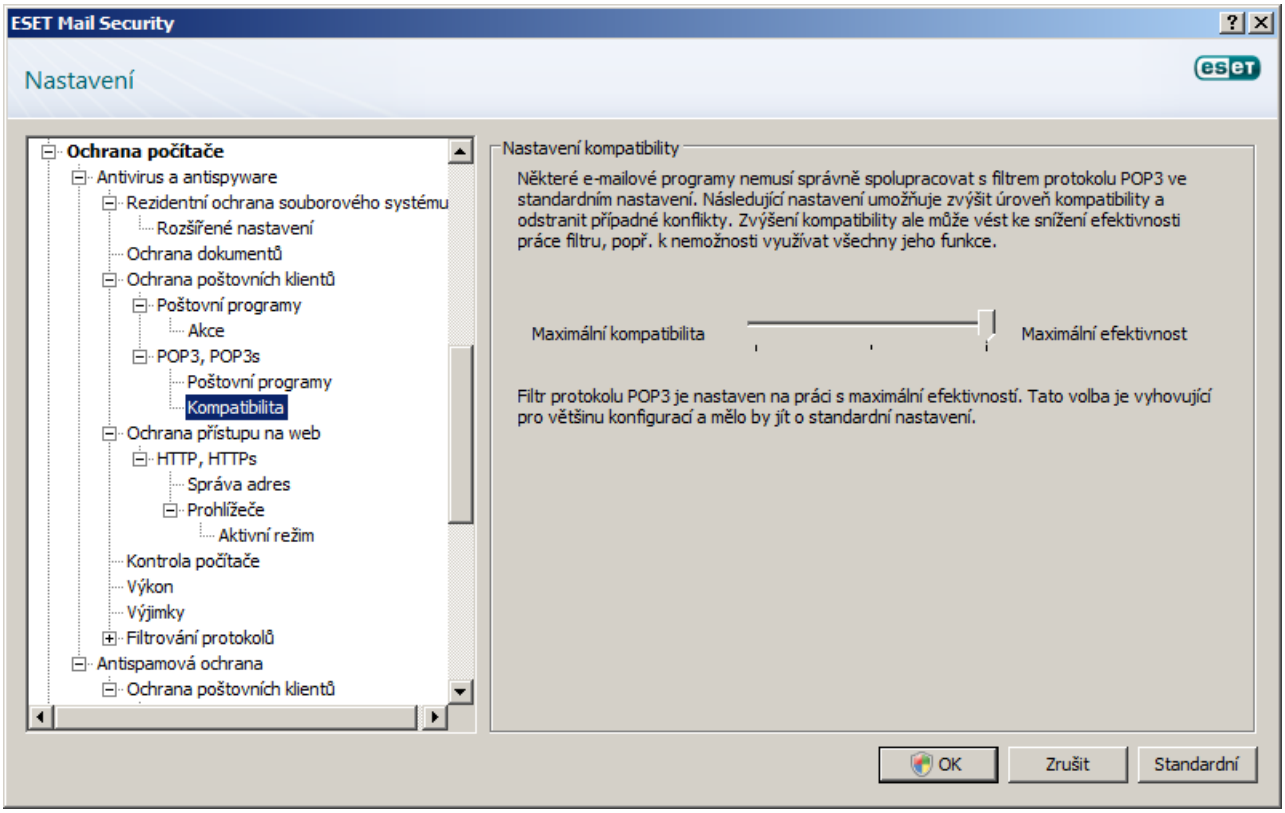
4.1.2.1.1 Kompatibilita

U některých poštovních klientů může nastat problém při přijímání zpráv (např. při příjímání zpráv pomocí pomalého internetového připojení dochází k uplynutí času určeného pro stáhnutí – timeoutu). V takových případech lze změnit způsob kontroly zpráv. Snížení úrovně bude mít vliv i na odstranění infiltrací ze zpráv.

Při **maximální efektivnosti** bude z infikované zprávy odstraněna (při výběru možnosti Smazat, Léčit nebo při nastavení maximální nebo střední úrovně léčení) infiltrace a do těla a předmětu zprávy bude přidána informace o infiltraci.

Při **střední úrovni** se změní způsob přijímání zpráv. Zprávy budou postupně předávány e-mailovému klientovi a až při přijímání poslední části bude zpráva zkontrolována na přítomnost infiltrace. U tohoto způsobu existuje riziko průniku infiltrace. Úroveň léčení a přidávání informací do předmětu a těla zprávy zůstává stejná jako při maximální efektivnosti.

Při **maximální kompatibilitě** bude uživatel pouze informován varovným oknem o tom, že mu byla doručena infikovaná zpráva. Doručená zpráva nebude obsahovat v předmětu a těle zprávy informace o detekci infiltrace a infiltrace nebude ze zprávy odstraněna. Infiltraci bude muset smazat sám uživatel v poštovním klientovi.

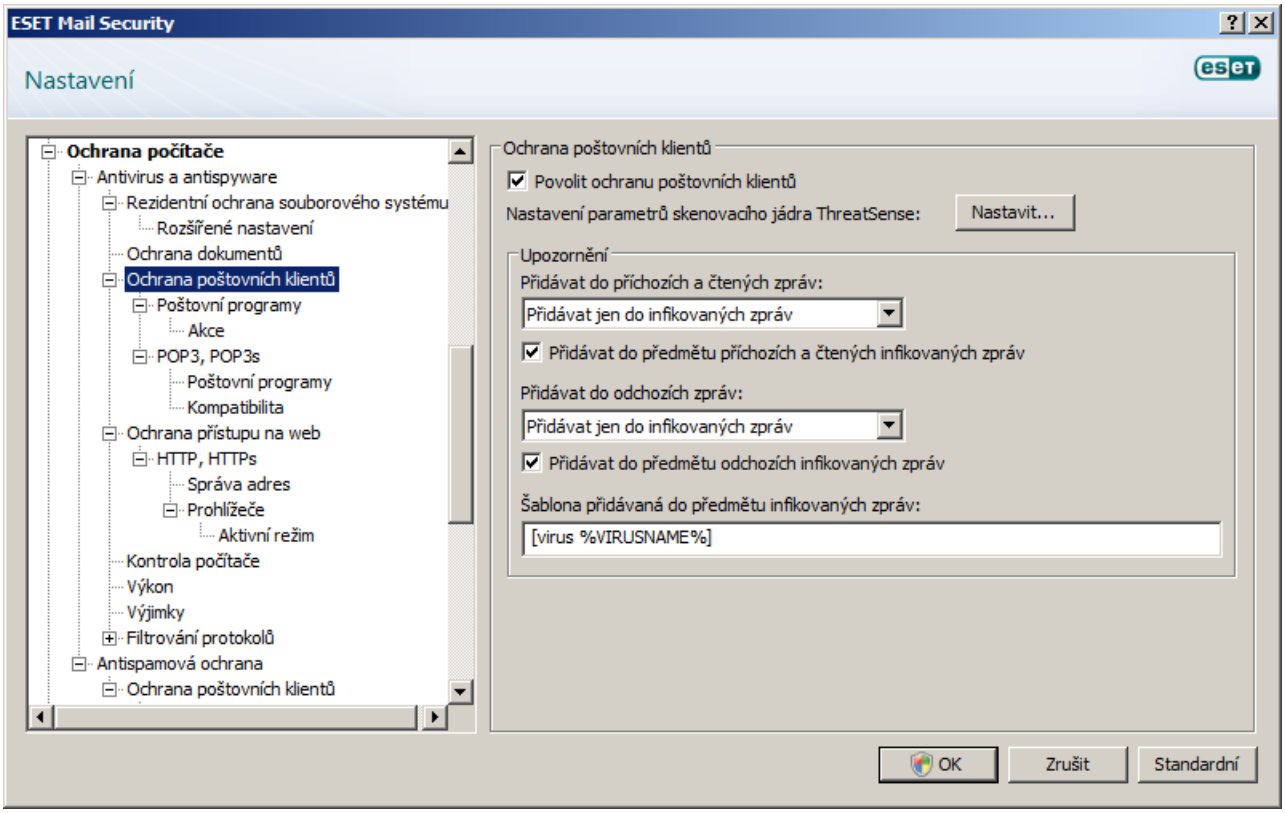


4.1.2.2 Integrace do poštovních klientů

Integrace ESET Mail Security a poštovních klientů zlepšuje možnost aktivní ochrany před škodlivým kódem v e-mailových zprávách. V případě, že je daný poštovní klient podporovaný, je vhodné povolit jeho integraci s ESET NOD32 Antivirus. Při integraci dochází přímo k vložení části ESET Mail Security do poštovního klienta, který přispívá k dokonalejší kontrole e-mailových zpráv. Konkrétní nastavení integrace jsou dostupná přes možnosti **Nastavení – Zobrazit celý strom pokročilých nastavení – Různé – Integrace s poštovními klienty**. V tomto dialogu je možné aktivovat integraci s podporovanými poštovními klienty, kteří jsou v současné verzi Microsoft Outlook, Outlook Express a Windows Mail, Windows Live Mail, Mozilla Thunderbird.

Volbu Vypnout kontrolu při změně obsahu složek s doručenou poštou doporučujeme použít v případě, že pociťujete zpomalení při práci s poštovním klientem. Uvedená situace může nastat například v případě přijímání zpráv z úložiště zpráv prostřednictvím Kerio Outlook Connectoru.

Ochrana elektronické pošty se zapíná příslušným zaškrtávacím tlačítkem v **Rozšířených nastaveních** ve větvi **Antivirus a antispyware** v podvětvi **Ochrana poštovních klientů.**



4.1.2.2.1 Přidávání upozornění do těla zprávy

Každá zpráva, kterou ESET Mail Security prověří, může být označena přidáním textu do předmětu nebo do textu zprávy. Tím zvyšujeme pro příjemce její důvěryhodnost a v případě zjištění infiltrace cennou informaci o nebezpečnosti dané e-mailové zprávy.

Možnosti nastavení této funkce jsou dostupné v **Rozšířených nastaveních** ve větvi **Ochrana počítače> Antivirus a antispyware> Ochrana poštovních klientů**. Textových upozornění **Přidávat do přijatých a čtených zpráv** i **Přidávat do odesílaných zpráv**. Obě tyto volby jsou doplněny nastavením, ve kterém uživatel rozhodne, zda chce přidávat do všech zpráv, infikovaných zpráv nebo nechce upozornění do těla zpráv přidávat vůbec.

Stejně je možné, aby ESET Mail Security přidával tato upozornění do předmětu infikované zprávy. Na to slouží volby **Přidávat do předmětu a čtených infikovaných zpráv** a **Přidávat do předmětu infikovaných zpráv**..

Obsah těchto upozornění v předmětu zpráv je povoleno modifikovat v položce **Šablona přidávaná do předmětu infikovaných zpráv**. Uvedená možnost umožňuje automatizovat proces zpracování varovných zpráv, což je přínosem zejména při kontrole většího počtu zpráv.

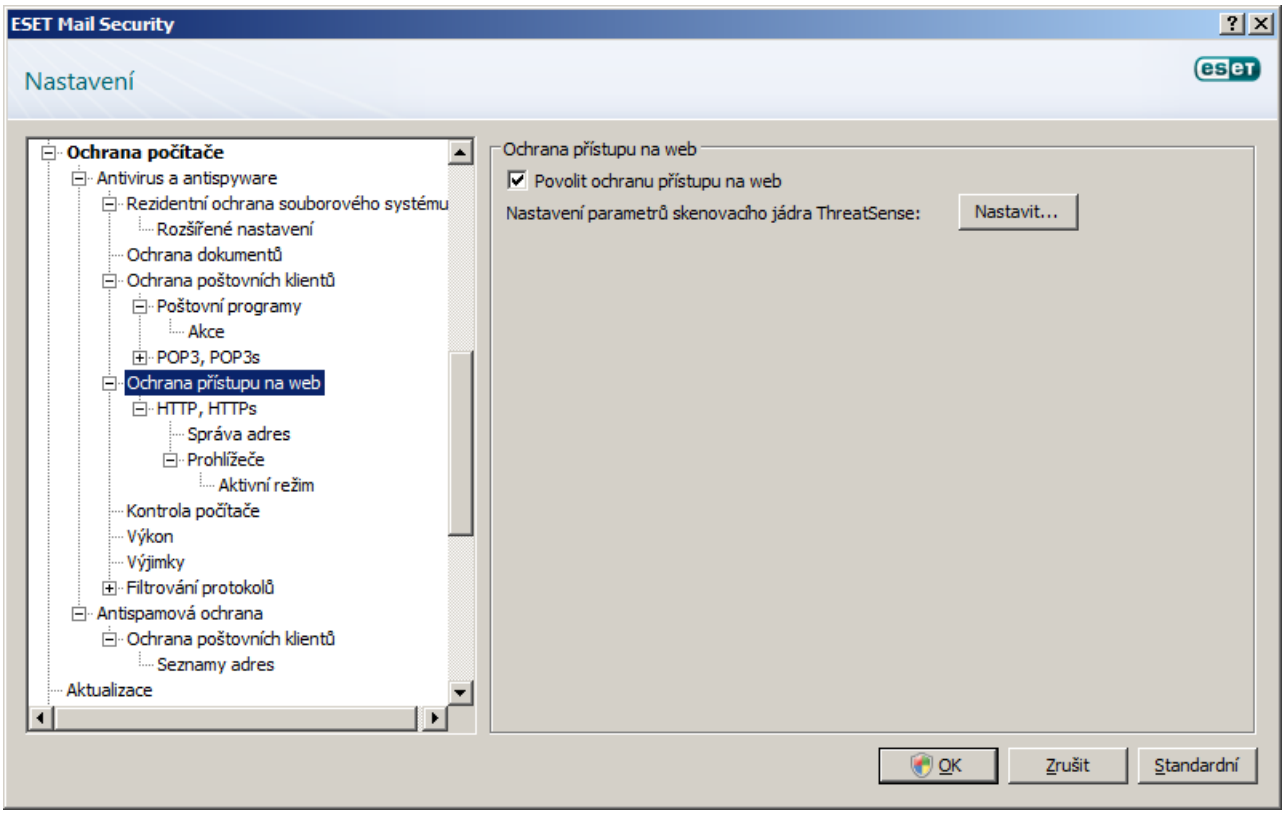
4.1.2.3 Odstranení infiltrace

Při příjmu infikovaného souboru se zobrazí varovné okno s informacemi o zjištění infiltrace. V okně jsou zobrazeny informace od koho byl e-mail doručen a jakou infiltraci obsahuje. V dolní části okna jsou zobrazeny akce, které lze s detekovaným objektem provést. Standardně doporučujeme vybrat akci **Léčit** nebo **Smazat**. Pokud ve výjimečných případech chcete, aby byl infikovaný soubor doručen, můžete zvolit akci **Ponechat**.

V případě nastavení **maximální úrovně** léčení je zobrazeno informační okno bez možnosti výběru akce, která se má s infikovaným objektem provést.

4.1.3 Ochrana přístupu na web

Internetové připojení patří do standardní výbavy osobních počítačů a bohužel se stalo i hlavním médiem přenosu škodlivého kódu. Tento fakt je hlavním důvodem, proč je třeba ochraně přístupu na web věnovat zvýšenou pozornost. Uživatelům se doporučuje mít aktivní volbu **Povolit ochranu přístupu na web** nacházející se v **Rozšířených nastaveních** ve větvi **Antivirus a antispyware > Ochrana přístupu na web**.



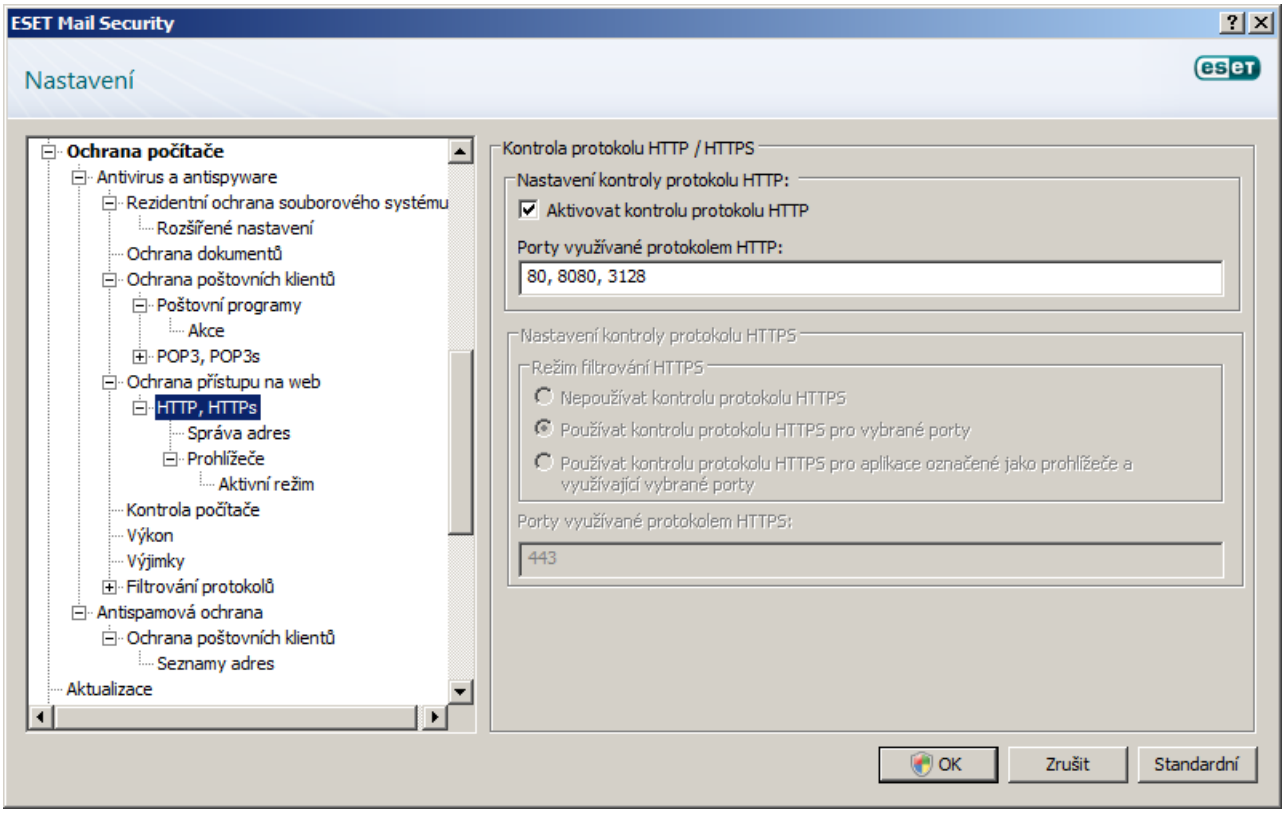
4.1.3.1 HTTP, HTTPs

Ochrana přístupu na web spočívá hlavně v monitorování komunikace prohlížečů internetových stránek ze servery, která probíhá podle pravidel protokolu HTTP, resp. HTTPs v případě šifrované komunikace. Konfigurace kontroly HTTP je napříč tomu možná z části **Ochrana přístupu na web**, položka **HTTP, HTTPs**. V hlavním okně konfigurace kontroly HTTP protokolu může uživatel tuto kontrolu aktivovat nebo deaktivovat možností **Aktivovat kontrolu protokolu HTTP**. Také je možné definovat čísla portů, na kterých v systému probíhá HTTP komunikace. Standardně jsou přednastavené hodnoty 80, 8080 a 3128.

Vedle standardní kontroly HTTP je možné aktivovat i kontrolu HTTPs (Hypertext Transfer Protocol Secure), který je zabezpečenou verzí protokolu HTTP. HTTPS šifruje přenos dat použitím SSL (Secure Socket Layer) protokolu čím zabezpečuje ochranu před odposlechem komunikace. Pro HTTPs komunikaci se standardně používá port 443. HTTPs je možné filtrovat ve dvou režimech:

Nepoužívat kontrolu protokolu HTTPs - Šifrovaná komunikace nebude kontrolována.

Používat kontrolu protokolu HTTPS pro vybrané porty - Kontrolovat se bude pouze komunikace přes porty definované v nastavení Porty používané protokolem HTTPs



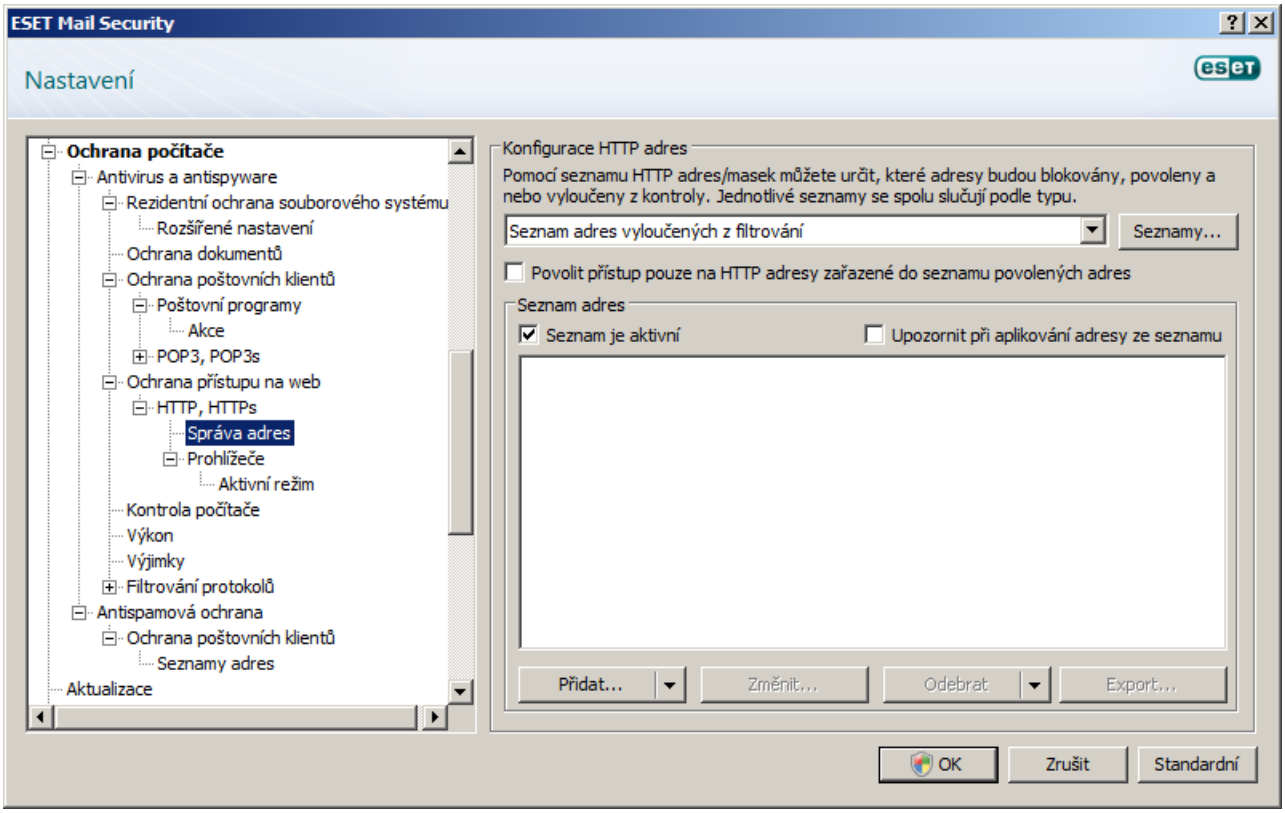
4.1.3.1.1 Správa adres

Kontrola protokolu HTTP ve svých nastaveních dovoluje definovat seznamy adres, které budou blokované, povolené nebo vyloučené z kontroly.

U každého seznamu jsou k dispozici tlačítka **Přidat, Změnit, Odebrat** a **Export**, které umožňují pohodlně spravovat a uchovávat seznam definovaných adres. V případě, že se uživatelům požadovaná adresa nachází v seznamu blokovaných adres, nebude přístup na tuto adresu povolen. Pokud je adresa aktivní v seznamu adres vyloučených z filtrování, bude zobrazená bez jakékoliv kontroly na škodlivý kód. Pokud se adresa nachází v seznamu povolených adres, bude na ni (a na další adresy v tomto seznamu) umožněn přístup pokud je aktivní volba **Povolit přístup pouze na HTTP adresy zařazené do seznamu povolených adres**. V seznam je možné používat speciální znaky * a ?, přičemž znak * nahrazuje libovolný řetězec a znak ? nahrazuje libovolný znak.

Aktivací seznamu zabezpečuje volba **Seznam je aktivní**. Při aplikování adresy ze seznamu je možné nastavit upozornění o této události prostřednictvím volby **Upozornit při aplikovaní adresy ze seznamu.**

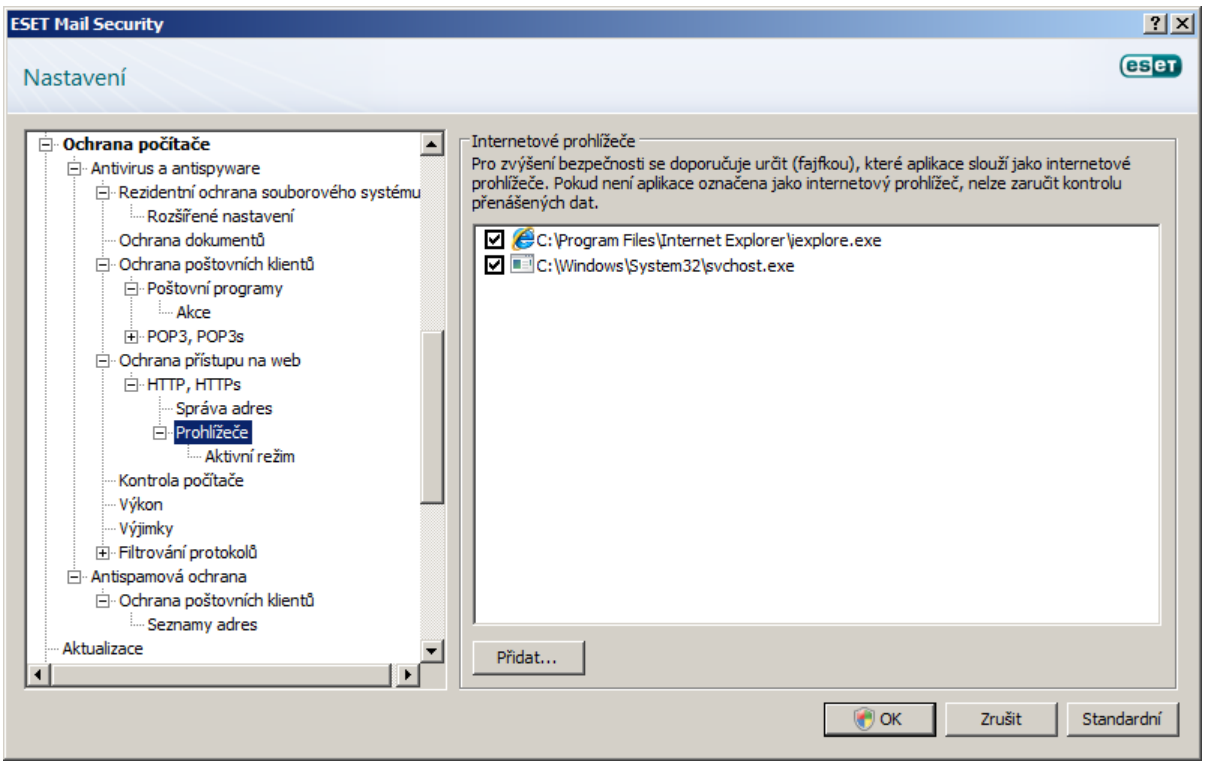
POZNÁMKA: Adresy vyloučené ze skenování se nekontrolují na hrozby a proto by měl seznam obsahovat pouze ověřené a důvěryhodné adresy. Také je potřeba dbát na opatrnost při používání speciálních znaků v tomto sezname, jejich nesprávné použití může omezit kontrolu komunikace z nedůvěryhodného serveru.



4.1.3.1.2 Aktivní režim internetových prohlížečů

Aplikace ESET Mail Security obsahuje funkci Prohlížeč, která umožňuje definovat, zda daná aplikace je nebo není prohlížeč. V případě, že aplikaci označíte jako prohlížeč, bude veškerá komunikace této aplikace monitorována bez ohledu na čísla portů, na kterých daná komunikace probíhá.

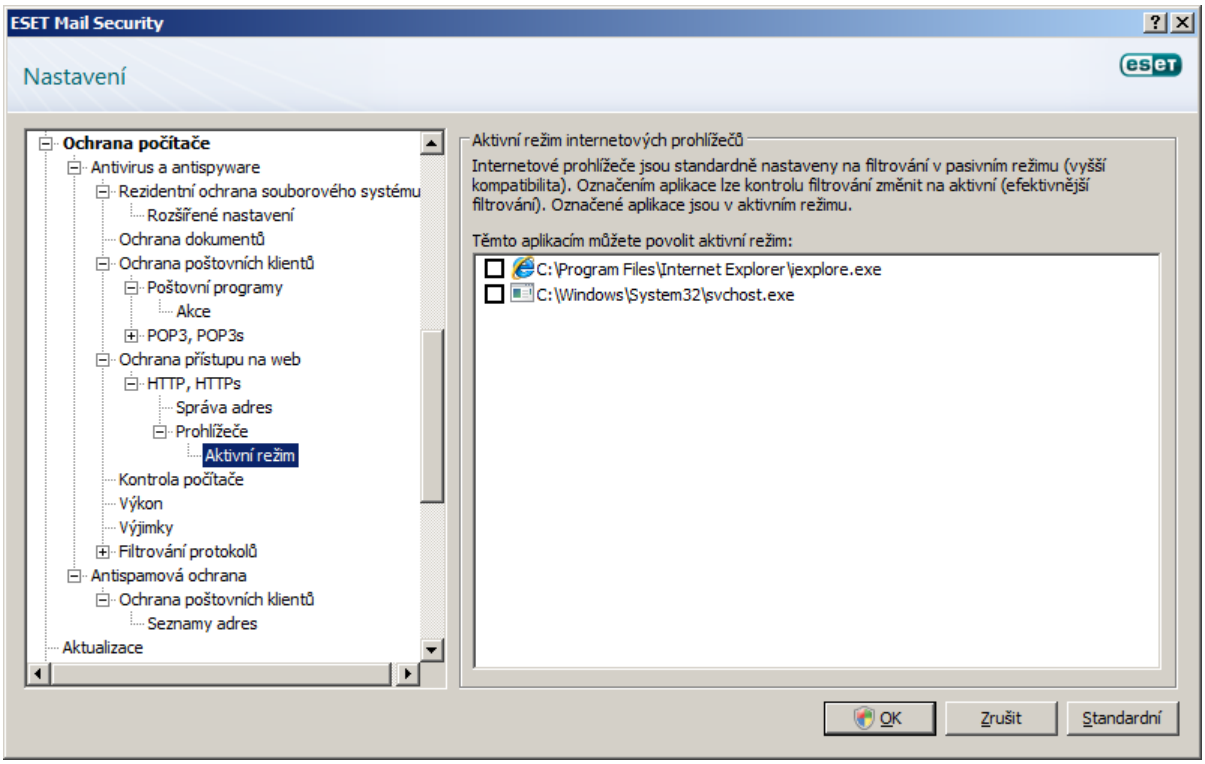
Funkce Prohlížeč představuje doplněk kontroly protokolu HTTP, která jinak probíhá jen na definovaných portech. Řada internetových služeb však využívá dynamicky se měnící nebo neznámá čísla portů a proto je potřeba mít možnost jejich kontroly bez ohledu na parametry spojení.



Seznam aplikací označených jako prohlížeče je k dispozici přímo z nastavení kontroly protokolu **HTTP, HTTPs** u možnosti Prohlížeče. Tato volba dále obsahuje položku **Aktivní režim**, která pro dané aplikace definuje režim jejich kontroly.

Aktivní režim nabízí účinnější kontrolu, protože přenášená data kontroluje jako celek. Není-li aktivní režimu použit, je komunikace aplikace monitorována postupně (po dávkách). To snižuje efektivitu kontroly, ale na druhé straně poskytuje vyšší kompatibilitu s aplikací. V případě, že při kontrole nedochází k potížím, doporučujeme používat aktivní režim kontroly.

POZNÁMKA: Na systémech Windows Vista se Service Packem 1 a Windows server 2008 je použit odlišný způsob kontroly komunikace (využívá se nová architektura Windows Filtering Platform) než na starších systémech. Z tohoto důvodu není nastavení Prohlížeče na těchto systémech dostupné.



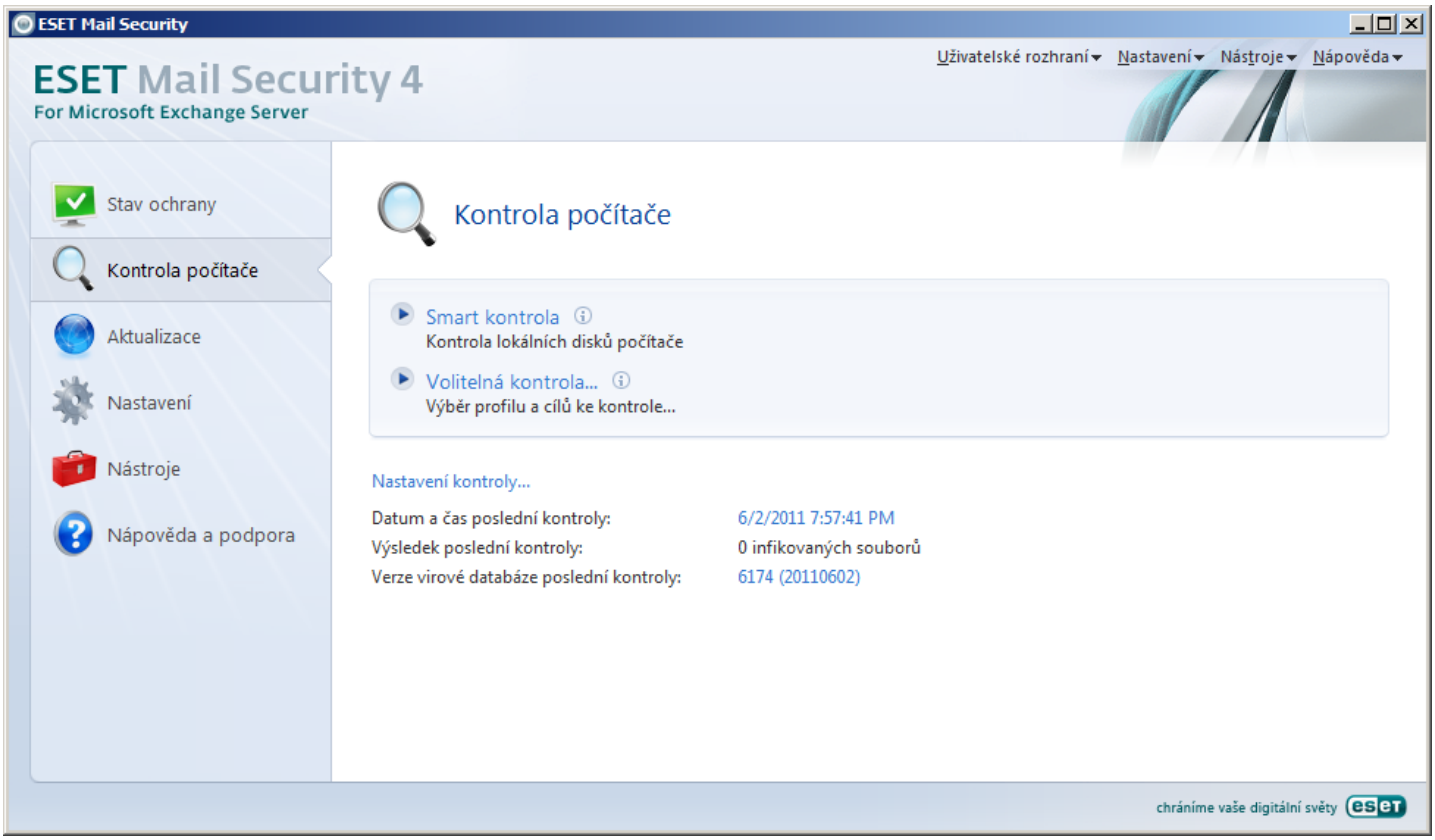
4.1.4 Kontrola počítače

Pokud máte podezření, že se v počítači může nacházet infiltrace (počítač se chová nestandardně), spusťte možnost Kontrola počítače. Tato možnost slouží k ověření přítomnosti infiltrace. Z bezpečnostního hlediska je žádoucí, aby kontrola počítače byla spouštěna nejen při podezření na infikované soubory, ale i průběžně v rámci prevence. Zajistí se tak detekce případných infiltrací, které nebyly v době zápisu na disk zachyceny rezidentní ochranou souborů. Taková situace může nastat zejména v případě, že byla rezidentní ochrana v té době vypnutá nebo virová databáze byla zastaralá. Doporučuje se, aby kontrola probíhala jednou za 1-2 měsíce.

Kontrolu lze nastavit také jako plánovanou úlohu v **Plánovači** (**Nástroje**).

4.1.4.1 Typy kontroly

Můžete si vybrat ze 2 typů kontroly. **Smart kontrola** slouží k rychlému spuštění kontroly počítače bez nastavování dalších parametrů kontroly. Druhým typem kontroly je **Volitelná kontrola...**, která naopak umožňuje vybrat si z různých přednastavených profilů skenování a určit cíle kontroly.



4.1.4.1.1 Smart kontrola

Prostřednictvím Smart kontroly je možné zabezpečit kontrolu počítače a léčení infikovaných souborů bez nutnosti zásahu uživatele. Výhodou standardní kontroly je rychlé spuštění skenování, nic není potřeba nastavovat. Kontrolovány jsou všechny soubory na lokálních discích (s výjimkou e-mailových a archivních souborů). Detekované infiltrace budou automaticky vyléčeny nebo odstraněny. Úroveň léčení je automaticky nastavena na standardní hodnotu. Podrobnější informace o typu léčení získáte v kapitole Léčení 62.

4.1.4.1.2 Volitelná kontrola

Volitelná kontrola je užitečná v případě, že chcete vybrat konkrétní cíle kontroly a metody skenování počítače. Výhodou je možnost vlastního nastavení všech podrobností kontroly. Tato nastavení lze uložit do tzv. **profilů**. To je užitečné zejména v případě, že chcete provádět pravidelnou vlastní kontrolu počítače se svými oblíbenými nastaveními.

Cíle kontroly můžete vybrat buď pomocí výběrové nabídky tzv. rychlého výběru cílů nebo prostřednictvím zadání cesty k požadovanému cíli kontroly. Dále můžete nastavit 3 úrovně léčení kontrolovaných souborů. V případě, že máte zájem pouze o kontrolu souborů bez jejich následného léčení, můžete vybrat možnost **Kontrolovat bez léčení**.

4.1.4.2 Cíle

Cíle kontroly slouží k výběru souborů, adresátů a zařízení (disků), které mají být zkontrolovány skenerem.

Rychlým výběrem cílů z výběrové nabídky můžete určit souhrnné cíle kontroly:

Podle nastavení profilu – vykoná výběr cílů uložených v profilu

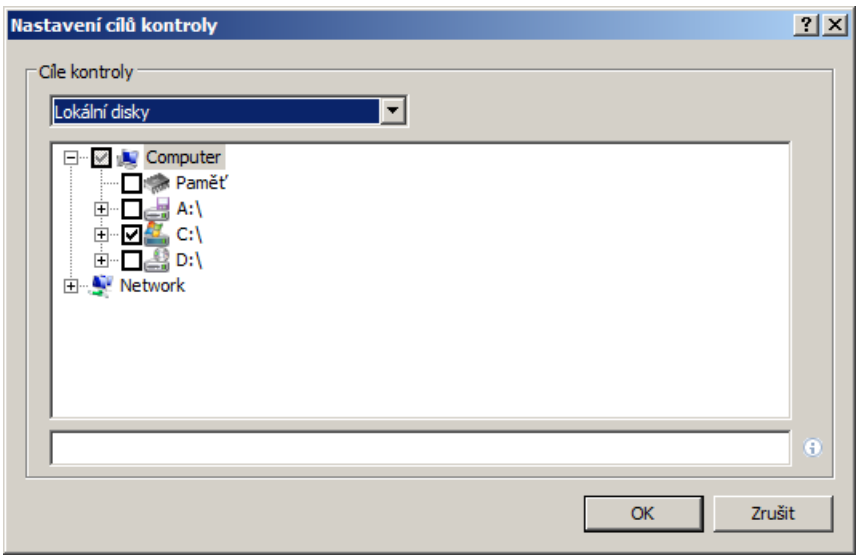
Výměnné disky – diskety, USB flash disky, paměťové karty, CD/DVD

Lokální disky – lokální pevné disky v počítači

Síťové disky – mapované disky

Bez výběru – zruší každý nastavený výběr

Cíle kontroly je možné podrobněji specifikovat zadáním cesty k adresářům a souborům, které se mají zkontrolovat. K tomu slouží stromová struktura všech zařízení počítače.

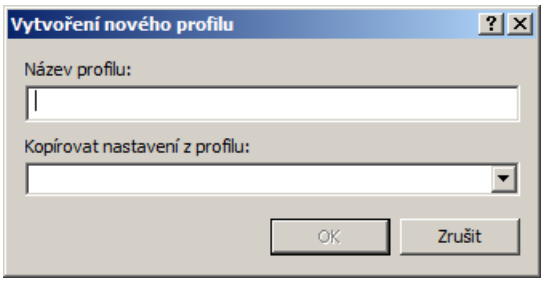


4.1.4.3 Profily

Oblíbené nastavení kontroly počítače lze uložit do profilů. Výhodou uložení nastavení do vlastního profilu skenování je jejich opakované využití v budoucnu. Je možné si vytvořit více profilů s různými cíli a metodami kontroly, případně s dalšími nastaveními.

Nový profil kontroly počítače, který budete později pravidelně spouštět například v rámci prevence počítače, vytvoříte v Rozšířených nastaveních ve větvi Kontrola počítače. V pravé části okna se nachází tlačítko **Profily...** Po klepnutí na něj se zobrazí seznam existujících profilů kontroly počítače s možností přidat nový. V části Nastavení skenovacího jádra ThreatSense 60 se nachází popis jednotlivých nastavení kontroly, který vám pomůže vytvořit si vlastní profil kontroly počítače podle vlastních preferencí.

PŘÍKLAD: Předpokládejme, že chcete vytvořit vlastní profil kontroly počítače a částečně vám vyhovují nastavení předdefinovaného profilu **Smart kontrola**. Nechcete však skenovat runtime archivy, zneužitelné aplikace a chcete použít přísné léčení. V takovém případě při vytváření nového profilu zvolte možnost nakopírovat do něj nastavení profilu **Smart kontrola**. Při úpravě nového profilu již zbývá jen upravit požadované rozdíly.



4.1.5 Výkon

V této části máte možnost nastavit počet skenovacích jader ThreatSense, které budou používány pro kontrolu počítače. Větší počet skenovacích jader na multi-procesorových serverech zvýší rychlost skenování. Akceptovaná hodnota pro toto nastavení je 1-20.

POZNÁMKA: Změna tohoto nastavení vyžaduje restart, aby bylo nové nastavení platné.

4.1.6 Filtrování protokolů

Kontrola protokolů POP3 a HTTP se provádí pomocí skenovacího jádra ThreatSense, které zahrnuje všechny pokročilé metody zjišťování škodlivého softwaru. Funguje nezávisle na použitém internetovém prohlížeči nebo poštovním klientovi. a když je aktivní (volba **Zapnout kontrolu aplikačních protokolů**), poskytuje 3 možnosti filtrování:

- **Pouze na základě portů pro HTTP a POP3** - při výběru této možnosti je kontrolována pouze komunikace probíhající na portech všeobecně používaných pro tyto služby.

- **Pouze pro aplikace označené jako internetové prohlížeče nebo poštovní klienti** - filtrována bude komunikace těch aplikací, které byly označeny jako prohlížeče nebo poštovní klienti

- **Na základě portů a aplikací označených jako internetové prohlížeče nebo poštovní klienti** - zahrnuje obě předcházející možnosti.

POZNÁMKA: Vzhledem k odlišnému způsobu filtrování komunikace na systémech Windows Vista se Service Packem 1 a Windows server 2008, není v sekci **Filtrování protokolů** dostupná žádná volba.

4.1.6.1 SSL

ESET Mail Security umožňuje i kontrolu protokolů zapouzdřených v protokolu SSL. Kontrolu je možné přizpůsobit podle toho, zda je certifikát využívaný danou SSL komunikací důvěryhodný, neznámý, nebo je v seznamu certifikátů pro které se nebude vykonávat kontrola obsahu v protokolu SSL.

Použít kontrolu protokolu SSL vždy (vyloučené a důvěryhodné certifikáty zůstanou platné) - při tomto nastavení se bude vykonávat kontrola každé komunikace přes protokol SSL kromě komunikace využívající certifikáty vyloučené z kontroly. Při komunikaci využívající zatím neznámý certifikát, který je důvěryhodně podepsán, nebude uživatel upozorněn na použití daného certifikátu a komunikace se bude automaticky filtrovat. Pokud uživatel přistupuje na server používající nedůvěryhodně podepsaný certifikát, přičemž byl uživatelem označený jako důvěryhodný (zařazený do seznamu důvěryhodných certifikátů), přístup bude povolen a komunikace bude filtrovaná.

Ptát se na nenavštívené stránky (možnost definovat výjimky)– v případě neznámého certifikátu bude zobrazené okno s možností výběru akce. Tento režim umožňuje vytvořit seznam certifikátů, pro které se nebude vykonávat kontrola v protokolu SSL.

Nepoužívat kontrolu protokolu SSL - nebude se používat filtrování komunikace přes protokol SSL.

4.1.6.1.1 Důvěryhodné certifikáty

Kromě úložiště důvěryhodných certifikátů, které ESET Mail Security obsahuje, má uživatel možnost označit i další certifikáty jako důvěryhodné. Ty jsou zobrazeny právě v seznamu **důvěryhodných certifikátů** v položce **Rozšířené nastavení (F5)** > **Ochrana počítače** > **Antivirus a antispyware** > **Filtrování protokolů** > **SSL** > **Certifikáty** > **Důvěryhodné certifikáty**.

4.1.6.1.2 Vyloučené certifikáty

V tomto seznamu se nacházejí certifikáty, které jsou považovány za bezpečné. Šifrovaná komunikace využívající certifikát z tohoto seznamu se nebude kontrolovat. Do seznamu můžou být zařazeny certifikáty stránek, které považujeme za bezpečné a není potřeba kontrolovat obsah.

4.1.7 Nastavení skenovacího jádra ThreatSense

ThreatSense je název technologie, která je tvořena souborem komplexních metod detekce infiltrace. Tato technologie je proaktivní, a proto poskytuje ochranu i během prvních hodin šíření nové hrozby. K odhalení hrozeb využívá kombinaci několika metod (analýza kódu, emulace kódu, generické signatury, virové signatury), čímž efektivně spojuje jejich výhody. Detekční jádro může kontrolovat několik datových toků paralelně a maximalizovat tak svůj výkon a účinnost detekce. Technologie ThreatSense dokáže účinně bojovat také s rootkity.

Pomocí nastavení ThreatSense lze nastavit podrobnosti kontroly:

- Typy souborů (podle přípon)
- Kombinace různých metod detekce
- Úrovně kontroly, atd.

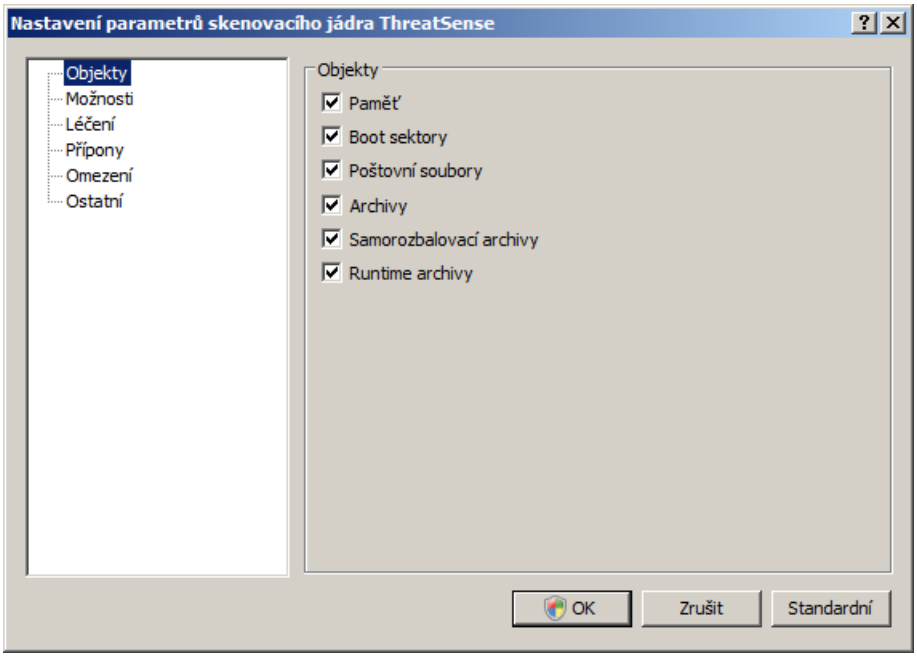
K nastavení se dostanete pomocí tlačítka **Nastavit...**, které naleznete v nastaveních příslušných modulů využívajících technologii ThreatSense. Pro různé druhy ochrany se používá různá úroveň nastavení. Technologii ThreatSense lze nastavit zejména pro následující moduly:

- Rezidentní ochrana souborového systému 46
- Kontrola souborů zaváděných při startu počítače (nastavitelná v nabídce **Rozšířené nastavení (F5)** > **Ochrana počítače** > **Antivirus a antispyware**)
- Ochrana poštovních klientů 49
- Ochrana přístupu na web 53
- Kontrola počítače 56

Jelikož jsou parametry ThreatSense maximálně optimalizovány pro každý modul,může modifikace značně ovlivnit činnost systému. Příkladem může být zpomalení systému při povolení kontroly **Runtime archivů** a rozšířené **Heuristiky** pro **Rezidentní ochranu** souborů (soubory jsou touto kontrolou kontrolovány pouze tehdy, pokud jsou nově vytvořené). Proto doporučujeme ponechat původní nastavení ThreatSense pro všechny druhy ochrany kromě **Rezidentní ochrany**.

4.1.7.1 Objekty kontroly

Položka **Objekty** umožňuje nastavit, které komponenty počítače a souborového systému budou testovány na přítomnost infiltrace.



Paměť – slouží ke skenování přítomnosti hrozeb, které můžou být zavedeny v operační paměti počítače.

Boot sektory – kontrola přítomnosti boot viru v sektorech disku, kde se nachází tzv. zaváděč operačního systému.

Soubory – skenování všech běžných typů souborů (programy, obrázky, audio, video, databázové soubory, atd.)

Poštovní soubory – skenování speciálních souborů, v kterých se nachází stáhnutá elektronická pošta

Archivy –skenování souborů nacházejících se v archivních souborech (RAR, ZIP, ARJ, TAR,..).

Samorozbalovací archivy – skenování souborů nacházejících se v samorozbalovacích archívních souborech, typická je pro ně přípona EXE

Runtime archívy – tzv. komprimované spustitelné soubory (programy), na rozdíl od klasických archívů se dekomprimují po spuštění v paměti počítače (typicky UPX, ASPack, yoda, aj.).

4.1.7.2 Možnosti detekce

V **možnostech** detekce může uživatel vybrat metody, které se použijí při ověřování přítomnosti infiltrace. Zvolit je možné následující metody:

Vzorky – Detekce infiltrace na základě tzv. virových signatur. Umožňuje odhalit a pojmenovat známé infiltrace.

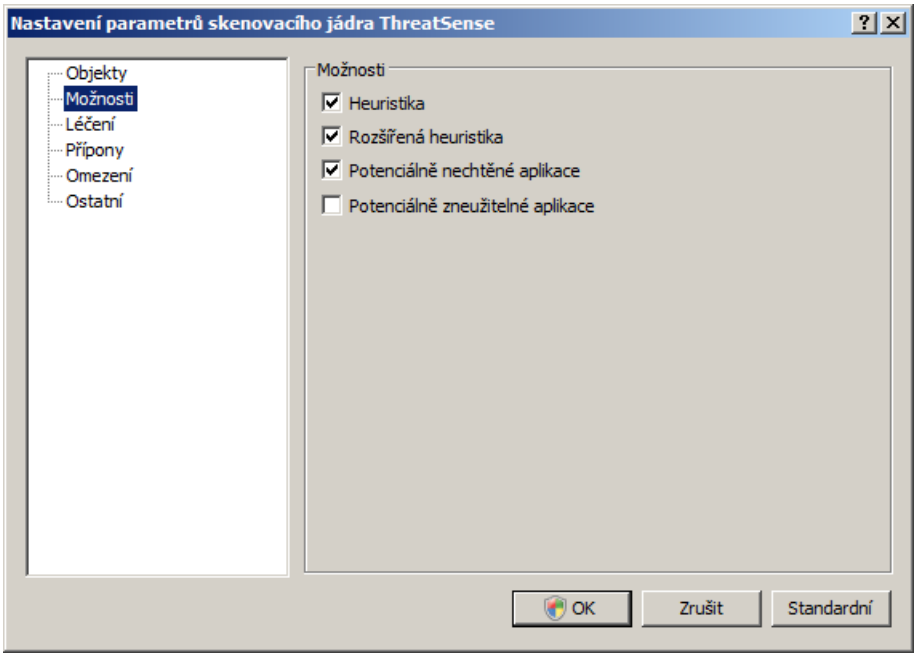
Heuristika – Ověřování přítomnosti hrozby pomocí analýzy činnosti programu. Výhodou heuristiky je schopnost odhalit i takový škodlivý software, který v době poslední aktualizace antivirového programu ještě neexistoval nebo nebyl znám.

Rozšířená heuristika – Jedinečný algoritmus heuristiky vyvinutý firmou ESET, který je optimalizován na odhalování červů a trojských koní vytvořených pomocí pokročilých programovacích jazyků. Rozšířená heuristika emuluje chování programů, čímž významně zlepšuje schopnost aplikace detekovat nové hrozby.

Adware/Spyware/Riskware – Software, který shromažďuje informace o uživateli a bez jeho vědomí je odesílá prostřednictvím internetu, jako je například software, který do počítače stahuje reklamu.

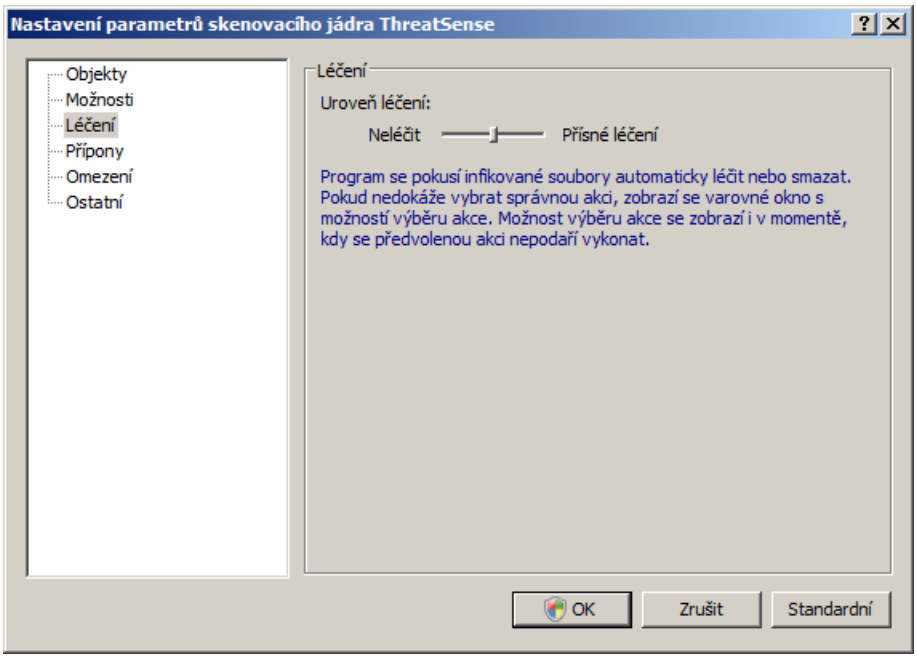
Potenciálně nechtěné aplikace – Programy, které sice nemusí představovat bezpečnostní riziko, avšak můžou mít určitý vliv na činnost počítačového systému. Tyto aplikace se obvykle do systému můžou nainstalovat až po souhlasu uživatele. Po této instalaci nastává určitě změna v chování systému v porovnání ze stavem před instalací této aplikace. Změnami v systému se rozumí zejména zobrazování oken, které by se jinak nezobrazovaly, aktivace a běh skrytých procesů, zvýšená spotřeba systémových prostředků, změny výsledků vyhledávání, komunikace se servery poskytovatele aplikace.

Potenciálně zneužitelné aplikace – Tato kategorie zahrnuje komerční software. Pokud je nainstalovaný bez vědomí uživatele, resp. správcem sítě. Jde většinou o programy pro vzdálenou správu sítě a proto je standardně tato možnost vypnutá.



4.1.7.3 Léčení

Určuje chování skeneru při léčení detekované infiltrace. K dispozici jsou 3 úrovně léčení:



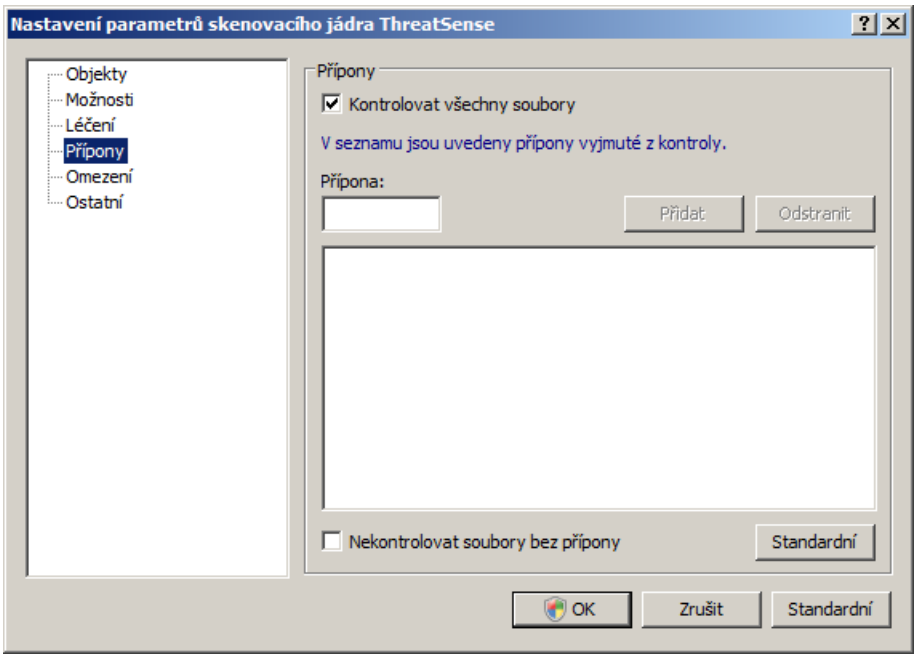
Neléčit
Infikované soubory nebudou automaticky léčené. Zobrazí se výstražné okno s možností výběru akce, která se má s danou infiltrací provést.
Standardní úroveň
Infikované soubory budou automaticky léčené nebo smazané. Pokud program neumí vybrat správnou akci, zobrazí se varovné okno s možností výběru akce. Toto okno se zobrazí i tehdy, pokud se předvolenou akci nepodaří provést.

Přísné léčení
Program vyléčí nebo smaže všechny infikované soubory (včetně archivů). Výjimkou jsou systémové soubory – pokud tyto soubory nelze léčit, je nabídnuta akce, která má být provedena.

UPOZORNĚNÍ: Při detekci infiltrace v archivním souboru bude archiv při standardní úrovni léčení odstraněn jen v případě, že obsahuje pouze infiltraci. Pokud archiv obsahuje i legitimní soubory, nebude odstraněn. V případě detekce infiltrace v archivu v režimu přísného léčení bude archivní soubor odstraněn i v případě, že obsahuje i bezpečné soubory.

4.1.7.4 Přípony

Přípona je část názvu souboru, zpravidla oddělená tečkou. Přípona určuje typ a obsah souboru. V této části nastavení ThreatSense zvolíte, které typy souborů budou kontrolované.



Přednastavena je kontrola všech souborů bez ohledu na příponu. Do seznamu souborů vyňatých z kontroly je možné přidat libovolnou příponu. V případě, že zrušíte zaškrtnutí políčka **Kontrolovat všechny soubory**, se seznam přípon změní na Seznam kontrolovaných přípon. V tomto seznamu se zobrazí předdefinované (nejčastější) typy souborů. Pomocí tlačítek **Přidat** a **Odstranit** povolíte nebo zakážete testování souborů s požadovanou příponou.

Chcete-li povolit kontrolu souborů bez přípony, je nutné zaškrtnou políčko **Kontrolovat soubory bez přípony**.

Vyloučení přípony z kontroly má smysl tehdy, pokud kontrola určitého typu souboru způsobuje nesprávné fungování programu, který s tímto typem přípony pracuje (např. vyloučení souborů typu EDB, EML a TMP při používání serveru MS Exchange).

4.1.7.5 Omezení

Omezení určující hranice velikostí objektů a archívů, které se budou testovat na přítomnost virů:

Maximální velikost objektu (v bytech)
Do uvedeného okénka má uživatel možnost definovat maximální hodnotu velikosti objektu. Daný modul antiviru bude kontrolovat pouze objekty s menší velikostí než je definovaná hodnota. Antivir standardně používá výrobcem předvolené hodnoty, které v mnohých případech není potřebné modifikovat. Tyto hodnoty doporučujeme modifikovat pouze pokročilým uživatelům, kteří chtějí velké objekty vyloučit z kontroly.

Maximální čas kontroly objektu (v sekundách)
Definuje maximálně povolený čas pro kontrolu objektů. Pokud si uživatel definuje určitou hodnotu, tak antivir při kontrole objektu po překročení této hodnoty ukončí probíhající kontrolu bez ohledu na kompletnost kontroly.

Úroveň vnoření archívů
Specifikuje maximální úroveň vnoření do archívu při kontrole antivirem. Antivir standardně používá výrobcem předvolenou hodnotu 10, kterou v mnohých případech není potřebné modifikovat. Pokud z tohoto důvodu dojde k předčasnému ukončení kontroly archívu, archív zůstane nezkontrolován.

Maximální velikost souboru v archívu (v bytech)
Specifikuje maximální velikost rozbaleného souboru v archívu, který se má kontrolovat. Pokud z tohoto důvodu dojde k předčasnému ukončení kontroly archívu, archív zůstane nezkontrolován.

4.1.7.6 Ostatní

Zapisovat všechna objekty do protokolu
Tato volba má rozdílný význam v nastavení rezidentní ochrany a v nastavení kontroly počítače. Při kontrole počítače aktivovaní této volby znamená, že do protokolů kontroly počítače budou zapsané všechny skenované soubory, včetně těch, které nebyly označené jako infikované. V případě rezidentní ochrany aktivování této volby znamená, že pokud se najde infiltrace v archivním souboru, budou do protokolu zaznamenané všechny soubory nacházející se v archívu, včetně těch, které nebyly označené jako infikované
.
V nastaveních kontroly počítače jsou k dispozici ještě tyto možnosti:

Kontrolovat alternativní datové proudy
Alternativní datové proudy (ADS) používané systémem NTFS jsou běžným způsobem neviditelné asociace k souborům a adresářům. Mnoho virů je proto využívá ke svému maskování před případným odhalením.

Kontroly na pozadí vykonávat s nízkou prioritou
Každá kontrola počítače využívá nezanedbatelný výkon procesoru. Jestliže právě pracujete s programy, náročnými na výkon procesoru, přesunutím kontroly na pozadí jim můžete přiřadit nižší prioritu a tím pádem zvýšit výkon pro Vaše aplikace.

Zachovat časy přístupu k souborům
Při kontrole souboru nebude změněný čas přístupu, ale bude ponechán původní (vhodné při používání zálohovacích systémů)
.
Rolování výpisu protokolu o kontrole
Umožňuje zapnutí / vypnutí rolování výpisu o kontrole. Pokud je rolování zapnuté, přímo úměrně s počtem kontrolovaných souborů narůstá i velikost protokolu o kontrole.

Zobrazovat informaci o ukončení kontroly v samostatném okně
Po ukončení kontroly budou zobrazeny informace v samostatném okně.

4.1.8 Detekce infiltrace

Infiltrace se mohou do počítače dostat z různých zdrojů: z webových stránek, ze sdílených adresářů, prostřednictvím e-mailu, z výměnných zařízení počítače (klíče USB, externí disky, disky CD a DVD, diskety a další).

Pokud je chování vašeho počítače podezřelé nebo máte podezření, že je infikován, postupujte následovně:

- Spusťte aplikaci ESET Mail Security a otevřete nabídku Kontrola počítače.
- Klikněte na tlačítko Smart kontrola 57
- Po ukončení kontroly se zobrazí protokol o kontrole, ve kterém je uvedený počet kontrolovaných, infikovaných a vyléčených souborů

Pokud program detekoval infiltraci, zachová se podle nastavené úrovně léčení modulu, který infiltraci odhalil (podrobnější informace naleznete v kapitole Léčení 62).

Předpokládejme například, že infiltraci zachytí rezidentní ochrana souborů, která má přednastavenou standardní úroveň léčení. V takovém případě se ochrana pokusí soubor buď vyléčit nebo smazat. Pokud rezidentní ochrana neví, jakou akci vybrat, zobrazí se uživateli výstražné okno, pomocí něhož vybere požadovanou akci. K dispozici jsou obvykle akce pro vyléčení, smazání a ponechání souboru. Možnost ponechat soubor se nedoporučuje, protože infiltrace zůstane zachována v původním umístění. Výjimkou je případ, kdy si je uživatel jistý, že infiltrace byla v souboru detekována omylem.

Léčení a smazání
Léčení souboru se dá aplikovat v případě, že do korektního souboru byla zavedena část, která obsahuje škodlivý kód. V takovém případě má smysl zkusit infikovaný soubor léčit a obnovit tak původní nezávadný soubor. V případě, že infiltrací je soubor obsahující výlučně škodlivý kód, bude příslušný soubor smazán.

Pokud je infiltrovaný soubor blokovaný například systémovým procesem, nebude soubor smazán ihned, ale až po restartu počítače.

Mazání souborů v archivech
Pokud je zjištěna infiltrace, která je sbalena v archivním souboru, bude archiv při standardní úrovni léčení smazán jen v případě, že obsahuje pouze soubor infiltrace. Pokud však archiv kromě infiltrace obsahuje i nezávadné soubory, nebude smazán. Při nastavení přísné úrovně léčení je třeba postupovat opatrně – v tomto případě bude archiv smazán bez ohledu na to, zda obsahuje i nezávadné soubory.

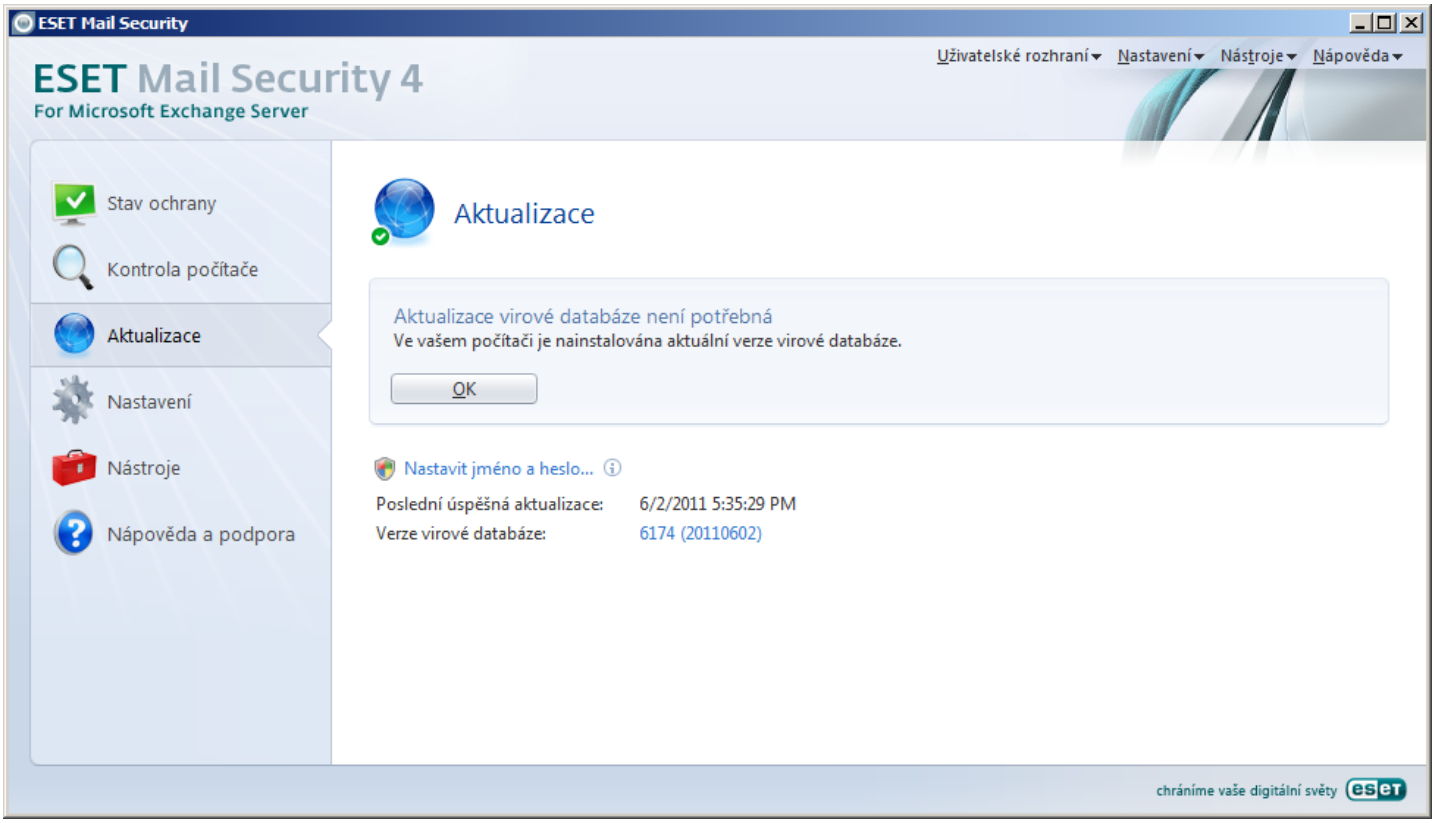
4.2 Aktualizace systému

Základním předpokladem pro maximální míru bezpečnosti poskytované aplikací ESET Mail Security je pravidelná aktualizace systému. Modul Aktualizace zabezpečuje, aby byla aplikace stále aktuální. Zabezpečuje přitom aktualizaci virových databází i aktualizaci všech komponent systému.

Informace o aktuálním stavu aktualizace jsou zobrazovány v položce **Aktualizace**. Obsahuje informace o tom, zda je virová databáze aktuální a zda je potřebná aktualizace.

Zároveň je nabídnuta možnost okamžité aktualizace odkazem **Aktualizovat virovou databázi** a také základní nastavení jako jméno a heslo pro autorizaci vůči aktualizačním serverům.

Prostřednictvím volby **Registrovat** je možné vyplnit online formulář, který zabezpečí registraci nové licence v databázi ESETu a následné poslání přihlašovacích údajů zákazníkovi.

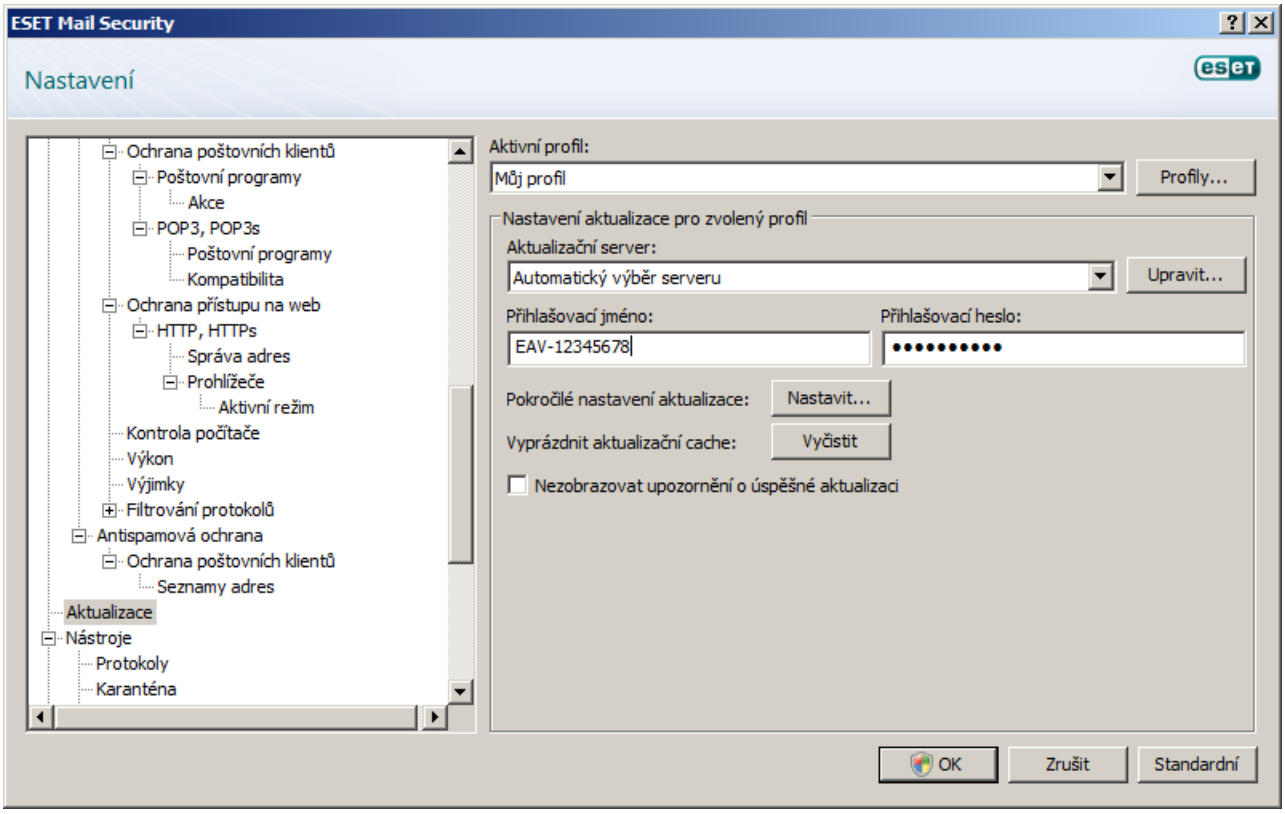


POZNÁMKA: Aktualizační jméno a heslo jsou přiděleny společností Eset po zakoupení licence produktu ESET Mail Security.

Informační okno kromě toho obsahuje informace o datu a čase poslední úspěšné aktualizace a číselné označení verze virové databáze. Toto číselné označení je zároveň aktivní odkaz na stránku společnosti Eset s informacemi o přidaných vzorcích v rámci dané aktualizace.

4.2.1 Nastavení aktualizace

Nastavení aktualizace se skládá z určení zdroje aktualizace, tj. z nastavení aktualizačních serverů a autorizace vůči těmto serverům. Standardně je Aktualizační server přednastavený na možnost **Automatický výběr serveru**. Toto nastavení zajistí aktualizaci z některého z aktualizačních serverů společnosti ESET, se zřetelem na momentální zatížení jednotlivých aktualizačních serverů. Konfigurace aktualizace je přístupná ve stromu **Pokročilých nastavení (F5)** ve větvi **Aktualizace**.

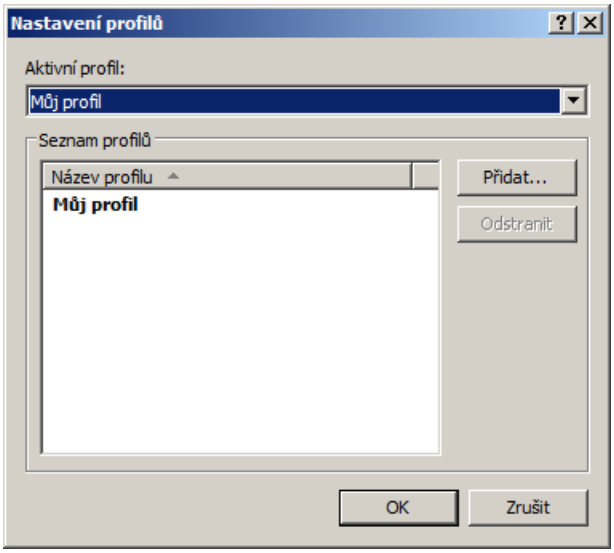


Seznam existujících aktualizačních serverů je k dispozici v rozevíracím seznamu **Aktualizační server**. Přidat nový server je možné tlačítkem **Upravit** v části **Nastavení** aktualizace pro zvolený profil a potom tlačítkem **Přidat**.

4.2.1.1 Aktualizační profily

Pro různá nastavení aktualizace je možné pro uživatele vytvářet definované profily, které se budou pro danou aktualizační úlohu používat. Vytvoření různých profilů pro aktualizaci má význam zejména pro mobilní uživatele (notebook nebo počítač, u kterého se mění způsob připojení na Internet). Takový uživatel může změnou aktualizační úlohy dosáhnout toho, že v případě, kdy nelze provést aktualizaci s nastaveními v profilu My Profile, se použije nastavení definované v alternativním profilu.

V poli **Aktivní profil** je vždy zobrazen momentálně vybraný profil. Standardně je tato položka nastavena na hodnotu **My profile**. Vytvoření nového profilu je možné provést tlačítkem **Profily**, potom tlačítkem **Přidat** a nakonec zadáním vlastního **Názvu profilu**. Při vytváření nového profilu je možné Kopírovat nastavení z profilu



V rámci nastavení profilu lze každému profilu určit aktualizační server, prostřednictvím kterého se aktualizace provádí. Je možné vybrat ze seznamu serverů nebo přidat nový server. Seznam existujících aktualizačních serverů je k dispozici v rozevíracím seznamu **Aktualizační server**. Přidat nový server je možné tlačítkem **Upravit** v části **Nastavení aktualizace** pro zvolený profil a potom tlačítkem **Přidat.**

4.2.1.2 Pokročilé nastavení aktualizace

Pokročilá nastavení aktualizace jsou k dispozici pomocí tlačítka **Nastavit**. Pokročilým nastavením aktualizace se rozumí nastavení **Módu aktualizace**, **HTTP Proxy**, **LAN a Mirroru**.

4.2.1.2.1 Mód aktualizace

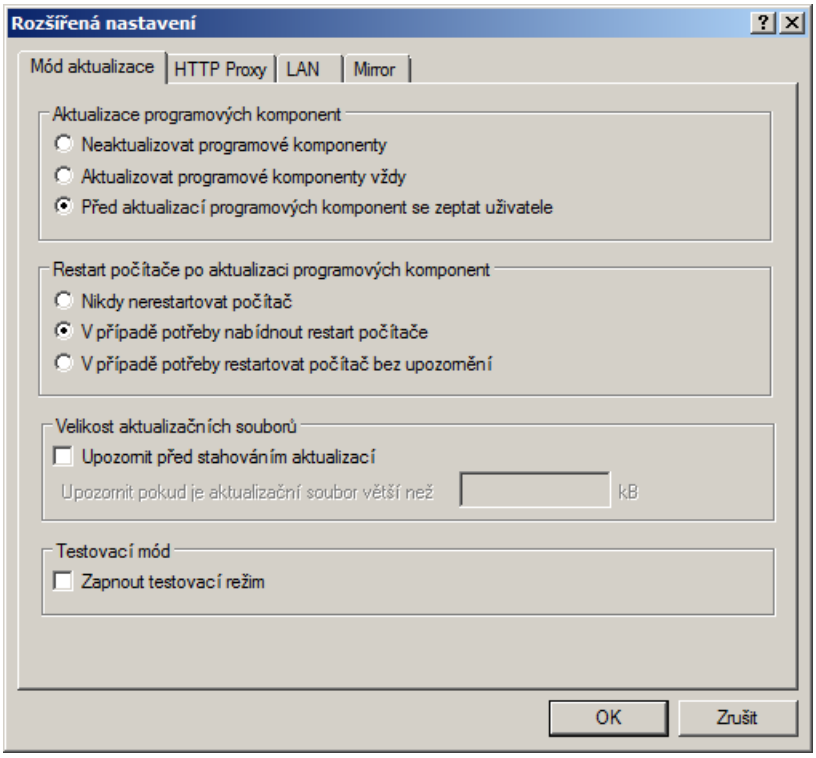
Na kartě **Mód aktualizace** se nachází nastavení související s aktualizací programových komponent.

V části **Aktualizace programových komponent** je možné vybrat ze tří možností:

- **Neaktualizovat programové komponenty**
- **Aktualizovat programové komponenty vždy**
- **Před aktualizací programových komponent se zeptat uživatele**

Možnost **Neaktualizovat programové komponenty** znamená, že při vydání aktualizace programových komponent společností ESET, spol. s r.o. nebude tato aktualizace stažena a neproběhne aktualizace komponent programu na dané stanici. Naopak, v případě možnosti **Aktualizovat programové komponenty vždy** se aktualizace programových komponent stáhne vždy, když bude pro danou verzi systému dostupná na aktualizačních serverech společnosti ESET, spol. s r.o., a komponenty programu budou aktualizovány na staženou verzi. Třetí možnost, **Před aktualizací programových komponent se zeptat uživatele**, uživateli zajistí možnost rozhodnout o aktualizaci programových komponent až v okamžiku, kdy bude tato aktualizace k dispozici. Zobrazí se dialogové okno s informacemi o dostupné aktualizaci programových komponent s možností potvrdit tuto aktualizaci nebo ji odmítnout. Podle toho, jak se uživatel rozhodne, se tato aktualizace stáhne a následně dojde k aktualizaci komponent.

Předvolená je při standardní instalaci možnost **Před aktualizací programových komponent se zeptat uživatele**.



Po aktualizaci programových komponent je nutné v zájmu plné funkčnosti modulů restartovat počítač. V části **Restart počítače po aktualizaci programových komponent** je možné vybrat ze tří možností:

- **Nikdy nerestartovat počítač**
- **V případě potřeby nabídnout restart počítače**
- **V případě potřeby restartovat počítač bez upozornění**

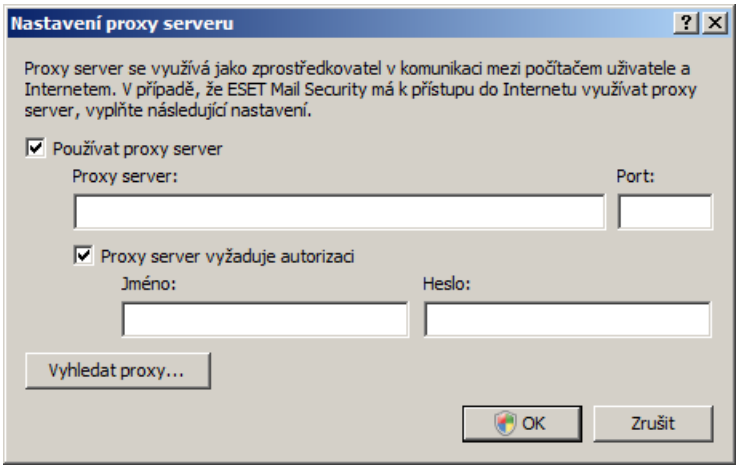
Při standardní instalaci je předvolena možnost **V případě potřeby nabídnout restart počítače**. Vhodnost použití jednotlivých voleb pro aktualizaci programových komponent v rámci karty **Mód aktualizace** závisí na stanici, na které budou uvedená nastavení použita. Zde je potřeba si uvědomit odlišnost nastavení při použití na serverech, kdy restart serveru v nevhodnou dobu není žádoucí.

4.2.1.2.2 Proxy server

Nastavení proxy serveru pro určitý aktualizační profil. Nastavení se nachází v **Pokročilých nastaveních aktualizace**, tj. pod položkou **Aktualizace** ve stromu pokročilých nastavení, potom klepněte na tlačítko **Nastavit** u možnosti Pokročilé nastavení aktualizace a na kartu **HTTP Proxy**. Při nastavení proxy serveru na této úrovni lze vybrat ze tří možností na kartě HTTP Proxy:

- **Použít globální nastavení proxy serveru**
- **Nepoužívat proxy server**
- **Spojení pomocí proxy serveru** (spojené s definováním podrobností takového připojení)

Možnost **Použít globální nastavení proxy** serveru použije celé nastavení proxy serveru, které už bylo definováno v položce **Různé**, ve větvi **Proxy server** ve zobrazení celého stromu pokročilých nastavení aplikace ESET Mail Security.

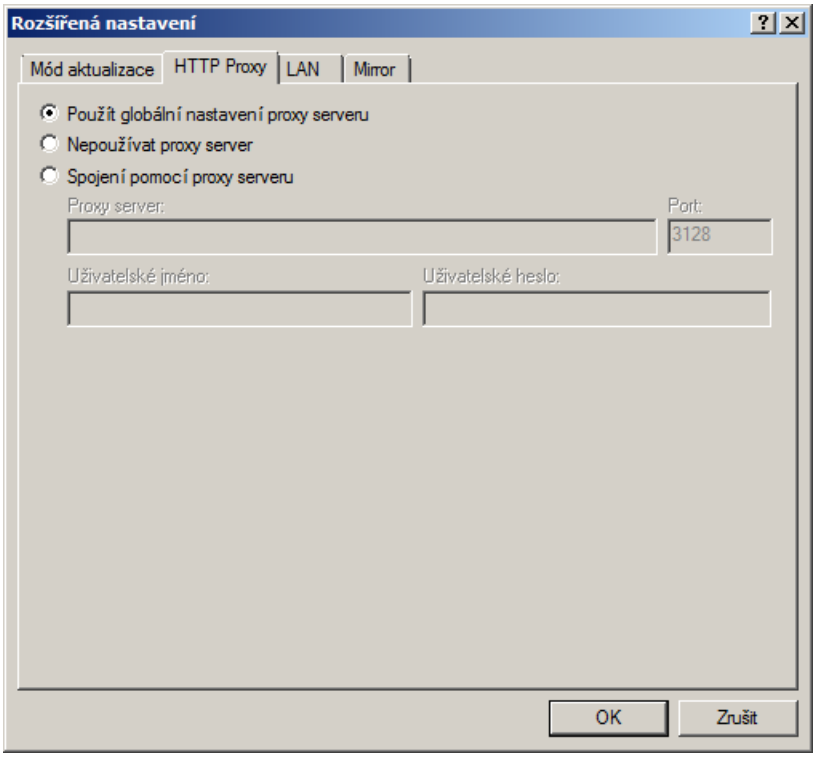


Možností **Nepoužívat proxy server** uživatel explicitně definuje, že při aktualizaci aplikace ESET Mail Security nemá být použit proxy server.

Možností **Spojení pomocí proxy serveru** uživatel definuje, že při aktualizaci aplikace ESET Mail Security bude použito spojení prostřednictvím proxy serveru, zároveň je však nutné definovat podrobnosti takového spojení, tj. adresu proxy serveru, komunikační port, resp. také jméno a heslo v případe potřeby autorizace vůči serveru.

Tato možnost se používá v případě, že proxy server používaný při aktualizaci aplikace ESET Mail Security možnost se používá v případě, že proxy server používaný při aktualizaci aplikace ESET Mail Security se bude používat spojení prostřednictvím proxy serveru.

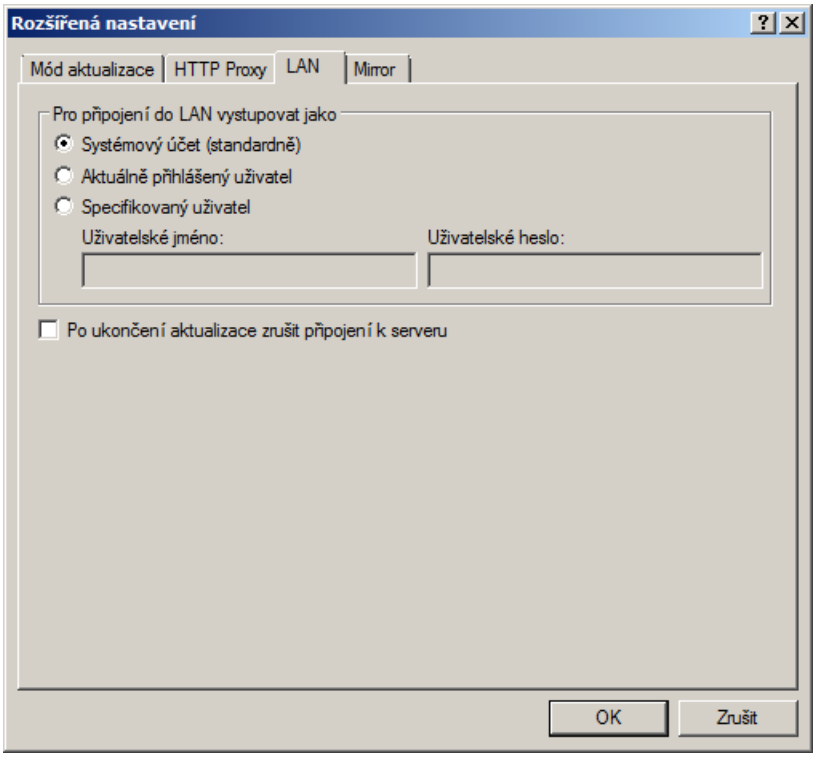
Ve výchozím nastavení je standardně vybraná možnost **Použít globální nastavení proxy serveru.**



4.2.1.2.3 Připojení do LAN

Při aktualizaci z místního serveru, na kterém je spuštěn systém NT, se k vytvoření připojení autorizace standardně vyžaduje. Ve výchozím nastavení nemá místní systémový účet definována práva pro přístup do adresáře s mirrorem (místní kopií aktualizačních souborů). V takovém případě je nutné v nastavení aktualizace zadat přístupové jméno a heslo, případně je potřeba určit účet, pod kterým bude aplikace přistupovat na server.

Nastavení tohoto účtu lze provést na kartě **LAN**. V části Pro připojení do LAN vystupovat jako jsou k dispozici možnosti **Systémový účet**, **Aktuálně přihlášený uživatel**, **Specifikovaný uživatel**.



Možnost **Systémový účet** způsobí, že se aplikace bude autorizovat pod systémovým účtem. Za normálních okolností autorizace neproběhne, pokud nejsou nastavené autorizační údaje v hlavních nastaveních aktualizace.

Možnost **Aktuálně přihlášený uživatel** způsobí, že se aplikace bude autorizovat pod účtem aktuálně přihlášeného uživatele. Nevýhodou tohoto nastavení je nemožnost připojení na server a následné aktualizace, pokud k počítači není přihlášen žádný uživatel.

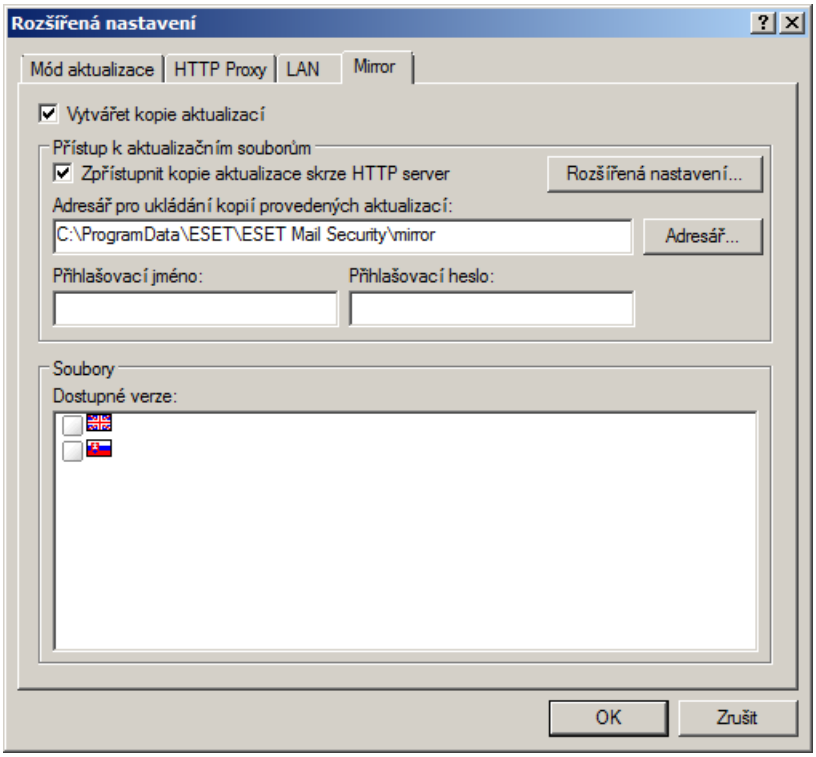
Možnost **Specifikovaný uživatel** zabezpečí autorizaci pod zadaným uživatelem.

Ve výchozím nastavení je standardně vybraná možnost **Systémový účet**.

4.2.1.2.4 Vytvoření kopie aktualizace - mirror

ESET Mail Security umožňuje vytvářet kopie aktualizace, s které lze aktualizovat další stanice v síti. Aktualizace stanic z mirroru zajistí rozložení zatížení sítě a také sníží zatížení internetového připojení.

Konfigurace vytváření mirroru je přístupná (po zadání licenčního souboru obdrženého při koupi produktu do lic. manažeru nacházejícího se v rozšířených nastaveních ESET Mail Security) v **Rozšířených nastaveních** aktualizace (ty zobrazíte prostřednictvím stromu Pokročilých nastavení aplikace ESET Mail Security a klepnutím na položku **Aktualizace**, na tlačítko **Nastavit** u možnosti **Pokročilé nastavení aktualizace** a na kartu **Mirror**).



Prvním předpokladem správného vytvoření mirroru je povolení této funkce v nastaveních, které je možné uskutečnit zaškrtnutím políčka **Vytvářet kopie aktualizací**. Zároveň se tím zpřístupní další nastavení mirroru, především způsob přístupu k aktualizačním souborům a definování adresáře, do kterého se budou ukládat aktualizační soubory vytvářeného mirroru.

Způsoby zpřístupnění mirroru jsou podrobněji probírány v části **Způsoby zpřístupnění mirroru**, proto jen ve stručnosti uvedeme, že existují dva základní způsoby zpřístupnění mirroru, a to buď prostřednictvím sdíleného adresáře nebo zpřístupněním kopie aktualizace přes server HTTP.

Adresář, do kterého se budou ukládat aktualizační soubory vytvářeného mirroru, se definuje v poli **Adresář, do kterého se budou ukládat kopie aktualizace**. Adresář je možné vyhledat v rámci adresářové struktury místního počítače a také v síti pomocí tlačítka **Adresář**. V případě, že k zápisu do zvoleného adresáře je nutná autorizace, je potřeba zadat autorizační údaje do polí Jméno a Heslo. Zadávají se ve tvaru Doména/uživatel nebo Pracovní_skupina/uživatel a s příslušnými hesly.

V definování mirroru může uživatel pokračovat až na úroveň definování jazykových verzí, pro které se má kopie aktualizace vytvořit. Nastavení jazykových verzí se provádí v části **Soubory** v poli **Dostupné verze**.

4.2.1.2.4.1 Způsoby zpřístupnění mirroru

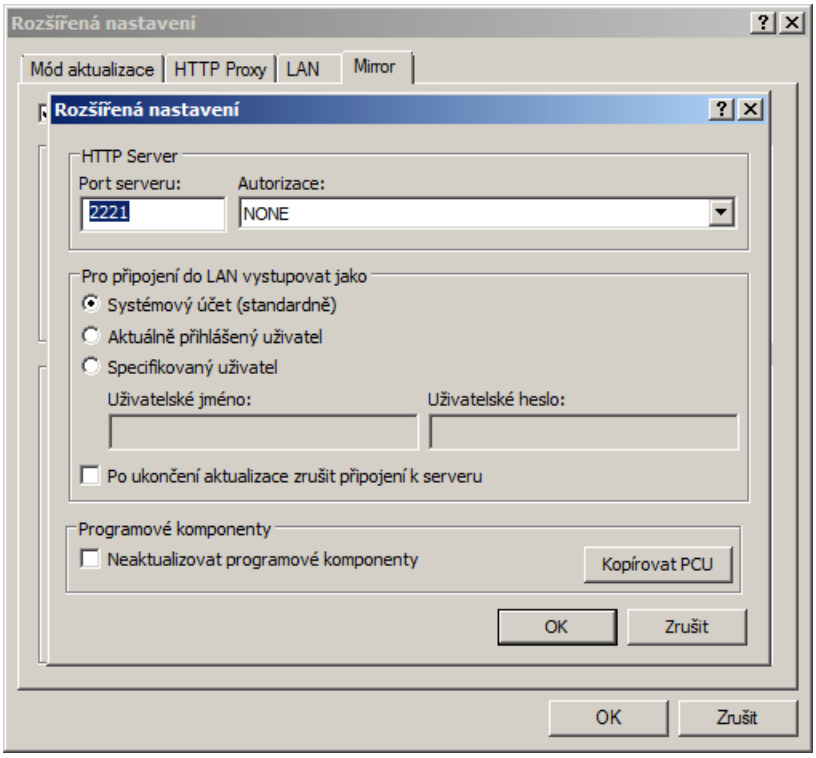
Existují dva základní způsoby zpřístupnění mirroru, a to pomocí sdíleného adresáře, nebo zpřístupněním kopie aktualizace přes HTTP.

Zpřístupnění mirroru pomocí HTTP serveru

Používá se automaticky jako předdefinované nastavení při standardní instalace, a proto ke zpřístupnění mirroru prostřednictvím HTTP serveru stačí v Rozšířených nastaveních aktualizace (na kartě **Mirror**) zaškrtnout políčko **Vytvářet kopie aktualizací**.

UPOZORNĚNÍ: Při zpřístupnění mirroru prostřednictvím HTTP serveru musí být mirror umístěn ve stejném počítači jako aplikace ESET Mail Security, která mirror vytváří.

Rozšířené nastavení umožňují nastavit **Port**, na kterém bude HTTP server naslouchat, a také typ **Autorizace** používané serverem. Při standardní instalaci je **Port serveru** předdefinovaný na **2221**. Pole Autorizace definuje metodu autorizace pro přístup ke sdíleným aktualizačním souborům. Možnost výběru ze tří položek **NONE**, **Basic**, **NTLM**. Položka **Basic** zajistí autorizaci pomocí jednoduché metody kódování base64. Položka **NTLM** zajistí kódování pomocí bezpečné metody. Při autorizaci se používají uživatelé vytvoření na stanici, která sdílí aktualizaci. Přednastavená je možnost **NONE**, která zpřístupňuje aktualizační soubory bez potřeby autorizace.



Po nastavení mirroru nastavíte na stanicích nový aktualizační server http://adresa_IP_vašeho_serveru:2221. Tuto operaci provedete takto:

- Otevřete okno Pokročilé nastavení aplikace ESET Mail Security a rozbalte větev **Aktualizace**
- V části **Aktualizační server** klepněte na tlačítko **Upravit** a přidejte nový server, http://adresa_IP_vašeho_serveru:2221
- V seznamu aktualizačních serverů vyberte přidaný server

Zpřístupnění mirroru pomocí sdíleného adresáře

Prvním předpokladem je vytvoření sdíleného adresáře na místním nebo síťovém disku. Při vytváření adresáře pro mirror je třeba dbát na to, aby uživatel, který do něj bude zapisovat, měl práva k zápisu a také aby uživatelé, kteří budou z mirroru provádět aktualizace, měli práva číst z adresáře mirroru. Pak je potřeba pokračovat v nastavování přístupu k mirroru v Rozšířených nastaveních aktualizace (na kartě **Mirror**), kde je nutné zrušit zaškrtnutí políčka **Zpřístupnit kopie aktualizace skrze HTTP server**, které je při standardní instalaci zaškrtnuto.

V případě umístění sdíleného adresáře na jiném počítači je nutné nastavit autorizaci vůči této stanici. Nastavíte ji v Rozšířených nastaveních aplikace ESET Mail Security pomocí možnosti Pro připojení do LAN vystupovat jako. Nastavení je totožné jako při aktualizaci a je popsané v kapitole Připojení do LAN 71.

Po nastavení mirroru nastavíme na stanicích nový aktualizační server \\UNC\CESTA. Postup je následující:

- Otevřete okno **Pokročilé nastavení** aplikace ESET Mail Security a rozbalte větev **Aktualizace**.
- V části **Aktualizační server** klepněte na tlačítko **Upravit...** a přidejte nový server, \\UNC\CESTA
- V seznamu aktualizačních serverů vyberte přidaný server

POZNÁMKA: Při zadávání cesty k aktualizačnímu serveru je důležité použít cestu ve tvaru UNC.

4.2.1.2.4.2 Problémy při aktualizaci z mirroru

Při aktualizaci z mirroru může v závislosti na nastavení přístupu k němu dojít k různým problémům. Většinou jsou problémy při aktualizaci z mirroru způsobené nesprávným definováním některého nastavení v rámci karty Mirror, nesprávným nastavením práv přístupu k aktualizačnímu adresáři **Mirror**, nesprávným nastavením místní stanice, která se pokouší provést aktualizaci z mirroru, nebo kombinací několika těchto příčin. Zde je přehled nejběžnějších problémů, k nimž může dojít při aktualizaci z mirroru:

- **ESET Mail Security nemůže navázat spojení s mirrorem** – Pravděpodobnou příčinou je nesprávné zadání aktualizačního serveru (síťové cesty k adresáři mirror), z kterého se má místní stanice aktualizovat. Správnost adresáře ověříte například tak, že klepnete na tlačítko Start, na příkaz Spustit , zadáte tento adresář a potvrdíte. Měl by se zobrazit obsah adresáře.
- **ESET Mail Security vyžaduje zadání jména a hesla** – Pravděpodobnou příčinou je nesprávné zadání autorizačních údajů (jména a hesla) v nastaveních aktualizace pro přístup na aktualizační server, z kterého se má místní stanice aktualizovat. Správnost těchto údajů proto také ověřte. Podle potřeby upravte položky tak, abyste dodrželi stanovenou formu zadávání těchto údajů, tj. Doména/jméno uživatele či Pracovní skupina/uživatelské jméno a příslušná hesla. Pokud je mirrorový adresář zpřístupněn pro všechny (Everyone), je třeba brát tento název s rezervou. Everyone neznamená libovolný anonymní přístup, ale pouze to, že je adresář přístupný všem uživatelům dané domény. Přestože je mirrorový adresář přístupný pro Everyone, je i tak nutné v nastaveních aktualizace zadat konkrétní doménové jméno uživatele s heslem.
- **ESET Mail Security nemůže navázat spojení s mirrorem** –Není povolená komunikace na portě, který byl definován pro zpřístupnění mirroru přes HTTP server.

4.2.2 Vytvoření aktualizační úlohy

Aktualizaci lze spustit manuálně potvrzením volby **Aktualizovat virovou databázi** v informačním okně zobrazeném po klepnutí na položku **Aktualizace**.

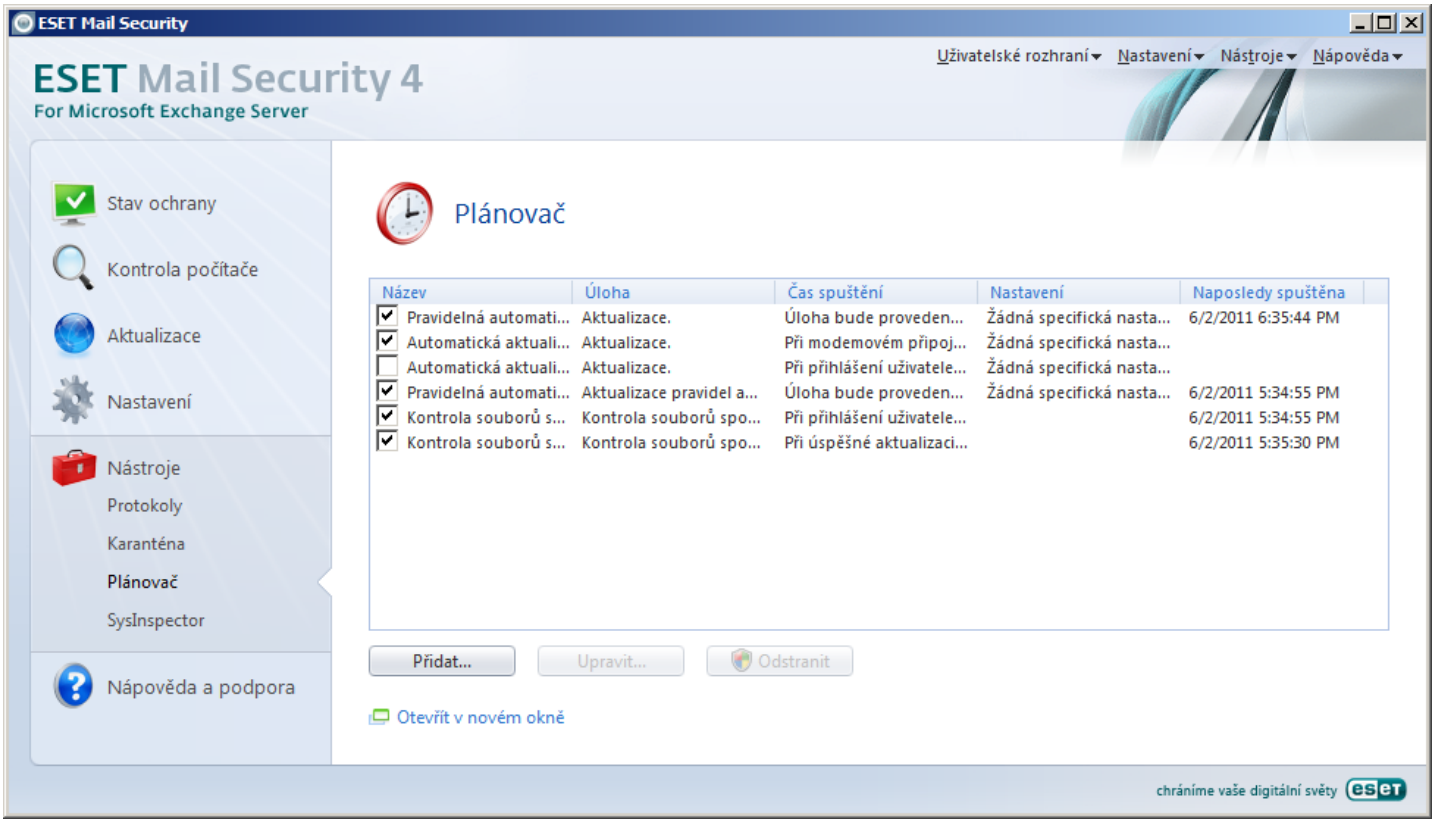
Aktualizaci je také možné spustit jako plánovanou úlohu, jejíž nastavení blíže určíte po klepnutí na příkaz **Plánovač** v nabídce **Nástroje**. Ve výchozím nastavení jsou při instalaci přidány tyto aktualizační úlohy:

- **Pravidelná automatická aktualizace**
- **Automatická aktualizace po modemovém spojení**
- **Automatická aktualizace po přihlášení uživatele.**

Každou z uvedených aktualizačních úloh může uživatel upravit podle svých potřeb. Kromě standardních aktualizačních úloh může uživatel vytvořit nové aktualizační úlohy s vlastním nastavením. Podrobněji je vytváření a nastavení aktualizačních úloh probíráno v kapitole Plánovač 75.

4.3 Plánovač

Plánovač je dostupný, je-li aktivní **Rozšířený režim** aplikace ESET Mail Security. V hlavní nabídce aplikace ESET Mail Security jej najdete jako položku nabídky **Nástroje**. Plánovač obsahuje přehledný seznam všech plánovaných úloh, jejich nastavení a vlastností, které se provádějí ve stanovený čas pomocí definovaných profilů.



Ve standardní instalaci zobrazuje **Plánovač** následujících pět plánovaných úloh:

- **Pravidelná automatická aktualizace**
- **Automatická aktualizace po modemovém spojení**
- **Automatická aktualizace po přihlášení uživatele**
- **Kontrola souborů spouštěných po spuštění při přihlášení uživatele k počítači**
- **Kontrola souborů spouštěných po spuštění při úspěšné aktualizaci virových databází**

Nastavení existujících plánovaných úloh (předdefinovaných i vlastních) je možné měnit příkazem Upravit z kontextové nabídky nebo výběrem příslušného řádku v seznamu úloh, který chcete změnit, a klepnutím na tlačítko **Upravit**. Podobně lze tlačítkem **Přidat** nebo **Odebrat** provést s vybranou úlohou příslušnou akci.

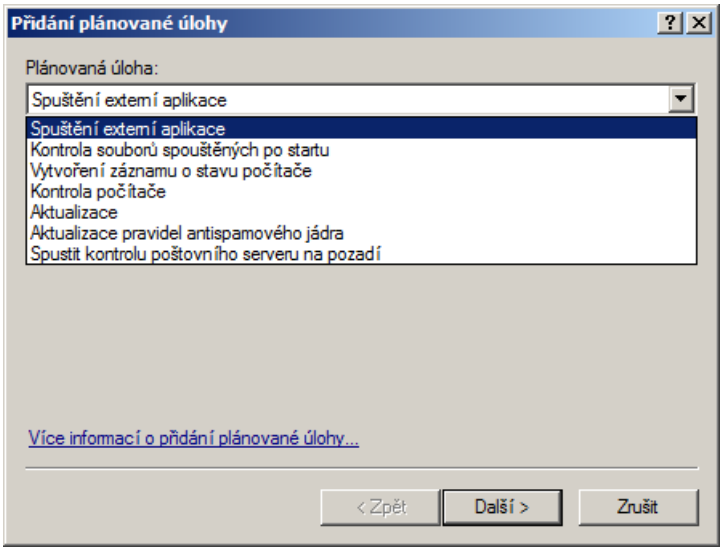
4.3.1 Kdy použít plánovač?

Plánovač slouží ke správě a provádění úloh s definovaným nastavením a vlastnostmi, které mají být provedeny ve stanovenou dobu a při jejichž použití mají být použity vybrané profily.

4.3.2 Vytvoření nové úlohy

Vytvoření nové úlohy v **Plánovači** je možné pomocí tlačítka Přidat nebo příkazem **Přidat** z kontextové nabídky. Můžete si vybrat z pěti typů plánovaných úloh:

- **Spuštění externí aplikace**
- **Kontrola souborů zaváděných při startu**
- **Kontrola počítače**
- **Aktualizace**



Mezi nejčastěji používané plánované úlohy patří **Kontrola počítače** a **Aktualizace**, proto si podrobněji popíšeme přidání aktualizační úlohy.

Po zobrazení nabídky plánovaných úloh tedy klepneme na možnost Aktualizace. Pokračujeme tlačítkem **Další**, do pole **Název úlohy** zadáme název úlohy a zvolíme periodicitu opakování úlohy. V souvislosti s periodicitou jsou k dispozici nastavení **Jednou**, **Opakovaně**, **Denně**, **Týdně**, Při **události** a další nastavení úlohy jsou odvozené od zvolené periodicity. Dále je třeba definovat akci, která se provede v případě, že ve stanoveném termínu nebude možné úlohu spustit. K dispozici jsou tři možnosti:

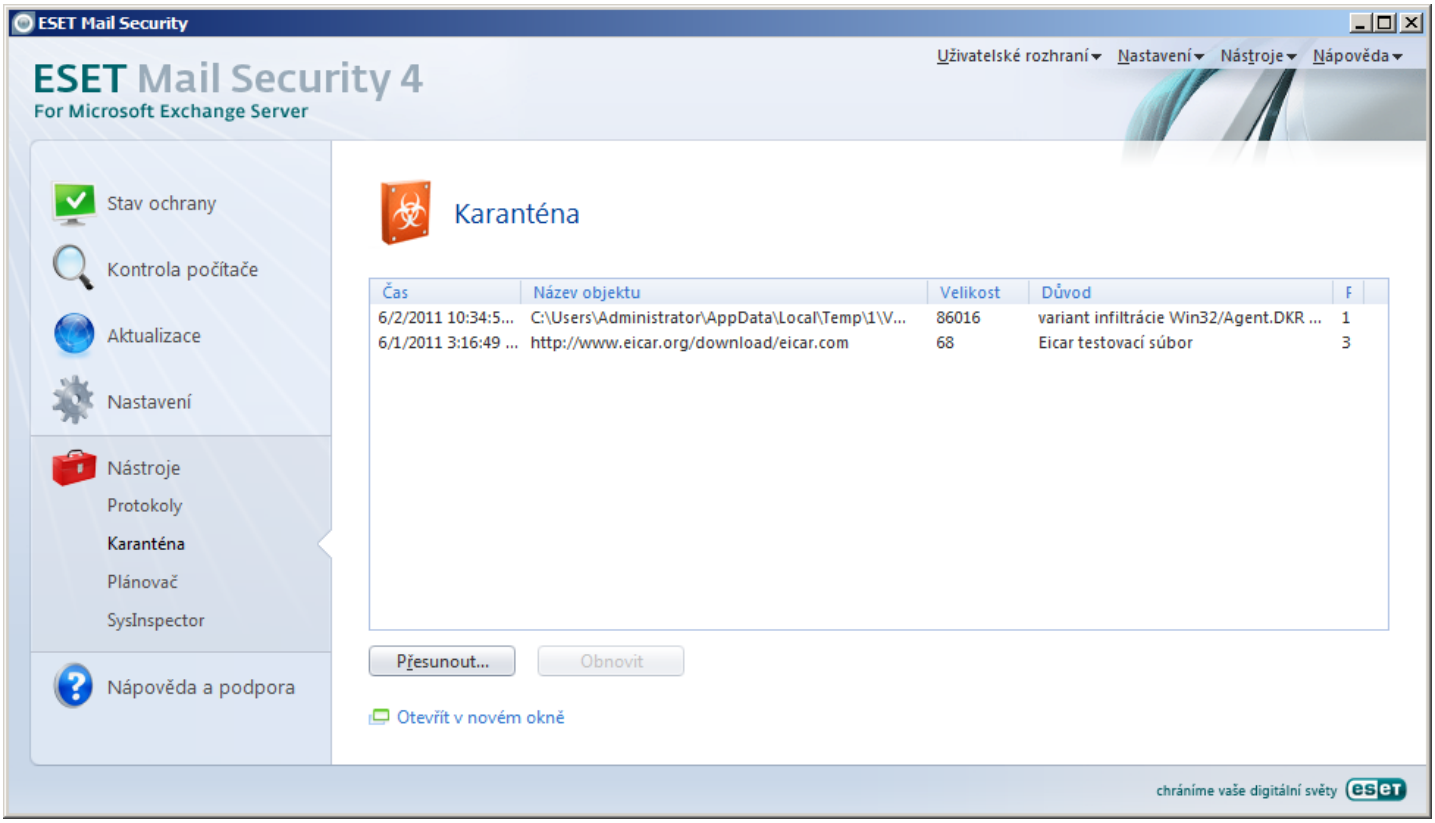
- **Provést úlohu v nejbližším naplánovaném termínu**
- **Provést úlohu hned, jakmile je to možné**
- **Vykonat úlohu hned, pokud od posledního provedení uplynul stanovený interval** (interval je možné definovat přímo při potvrzení této možnosti)

V dalším kroku jsou zobrazené kompletní informace o přidávané plánované úloze se zaškrtnutým políčkem **Při provedení úlohy zadat specifická nastavení**. Pouze pokud je políčko zaškrtnuté, jsou po klepnutí na tlačítko **Dokončit** v přidávané plánované úloze k dispozici nastavení profilů, která se mají při provádění úlohy použít. Je možné definovat primární a alternativní profil, který se použije v případě, že úlohu nebude možné provést pomocí primárního profilu. Potvrzením tlačítka **OK** v okně profilů se vytvořená plánovaná úloha přidá do seznamu plánovaných úloh.

4.4 Karanténa

Hlavní úlohou karantény je bezpečné uchovávání infikovaných souborů. Ve většině případů se může jednat o soubory, pro které neexistuje léčení, není jisté, zda je bezpečné je smazat, případně se jedná o nesprávnou detekci antivirové ochrany.

Soubory do karantény mohou být přidány i samotným uživatelem. Může k tomu dojít například v případě, že soubor není detekován antivirovým skenerem a má podezřelé chování. Soubory z karantény mohou být zaslány do virové laboratoře společnosti ESET.



Soubory uložené v karanténě si můžete prohlédnout v přehledné tabulce, kde jsou informace o datu a čase přidání souboru do karantény, cesta k původnímu umístění souboru, jeho délka v bajtech, důvod (**přidaný uživatelem...**), počet infiltrací (např. pokud archiv obsahoval více infikovaných souborů).

4.4.1 Přidání do karantény

ESET Mail Security přidává soubory do karantény automaticky při jejich mazání (pokud uživatel ve varovném okně nezruší tuto možnost). Pokud ovšem uživatel uzná za vhodné, může pomocí tlačítka **Přidat** uložit jakýkoli podezřelý soubor do karantény ručně. V takovém případě ovšem soubor nebude smazán ze svého původního umístění. Kromě tlačítka **Přidat** lze k tomuto účelu použít po klepnutí pravým tlačítkem myši na plochu karantény také kontextovou nabídku, ze které vyberete možnost **Přidat**.

4.4.2 Obnovení z karantény

Soubory uložené v karanténě lze vrátit do jejich původního umístění, odkud byly smazány. Slouží k tomu funkce **Obnovit**, která je také přístupná prostřednictvím kontextové nabídky po klepnutí pravým tlačítkem myši na daný soubor v karanténě. V kontextové nabídce je navíc možnost **Obnovit do**, která umožňuje obnovit soubor na jiné místo než to, ze kterého byl původně smazán.

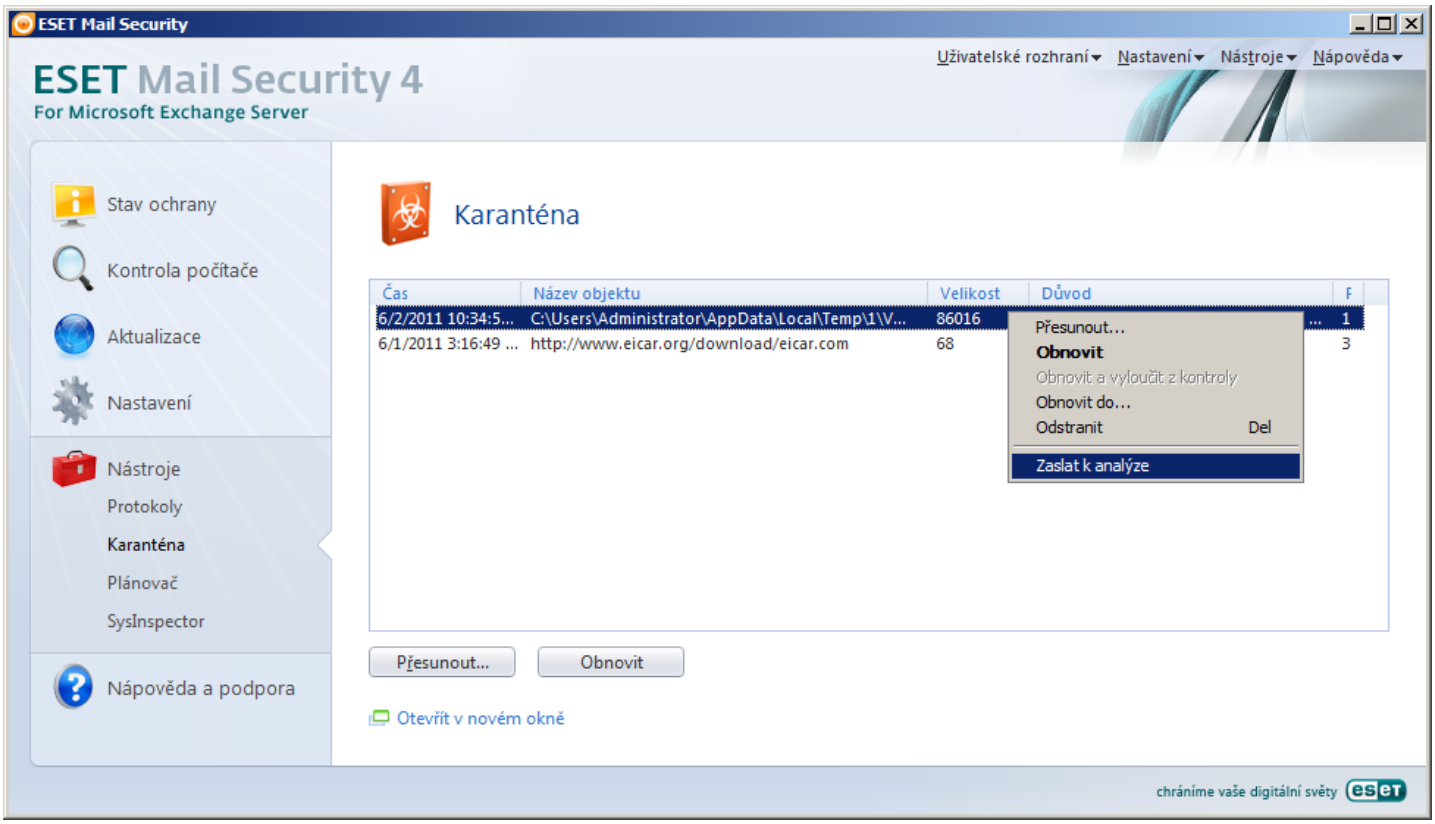
VAROVÁNÍ: Po obnovení souborů z karantény doporučujeme tyto soubory zkontrolovat a zjistit, zda neobsahují škodlivý kód.

POZNÁMKA: Pokud byl soubor do karantény přidán z důvodu falešného poplachu, je třeba jej po obnovení vyloučit z kontroly a zaslat technické podpoře společnosti ESET.

4.4.3 Poslání k analýze

Pokud jste uložili do karantény podezřelý soubor, který nebyl detekován, nebo pokud program nesprávně vyhodnotil soubor jako infikovaný (např. při heuristické analýze kódu) a umístil jej do karantény, zašlete tento soubor k analýze do virové laboratoře společnosti ESET. Klepněte na daný soubor v karanténě pravým tlačítkem myši a z kontextové nabídky vyberte možnost **Zaslat k analýze**. V zobrazeném okně vyplníte políčko komentář, kde můžete uvést stručné informace o viru (za jakých okolností se dostal na počítač, jak se projevuje, atd.), a políčko email, kde uvedete Vaši emailovou adresu, na kterou Vás v případě potřeby doplnění dalších informací mohou kontaktovat analytici společnosti ESET.

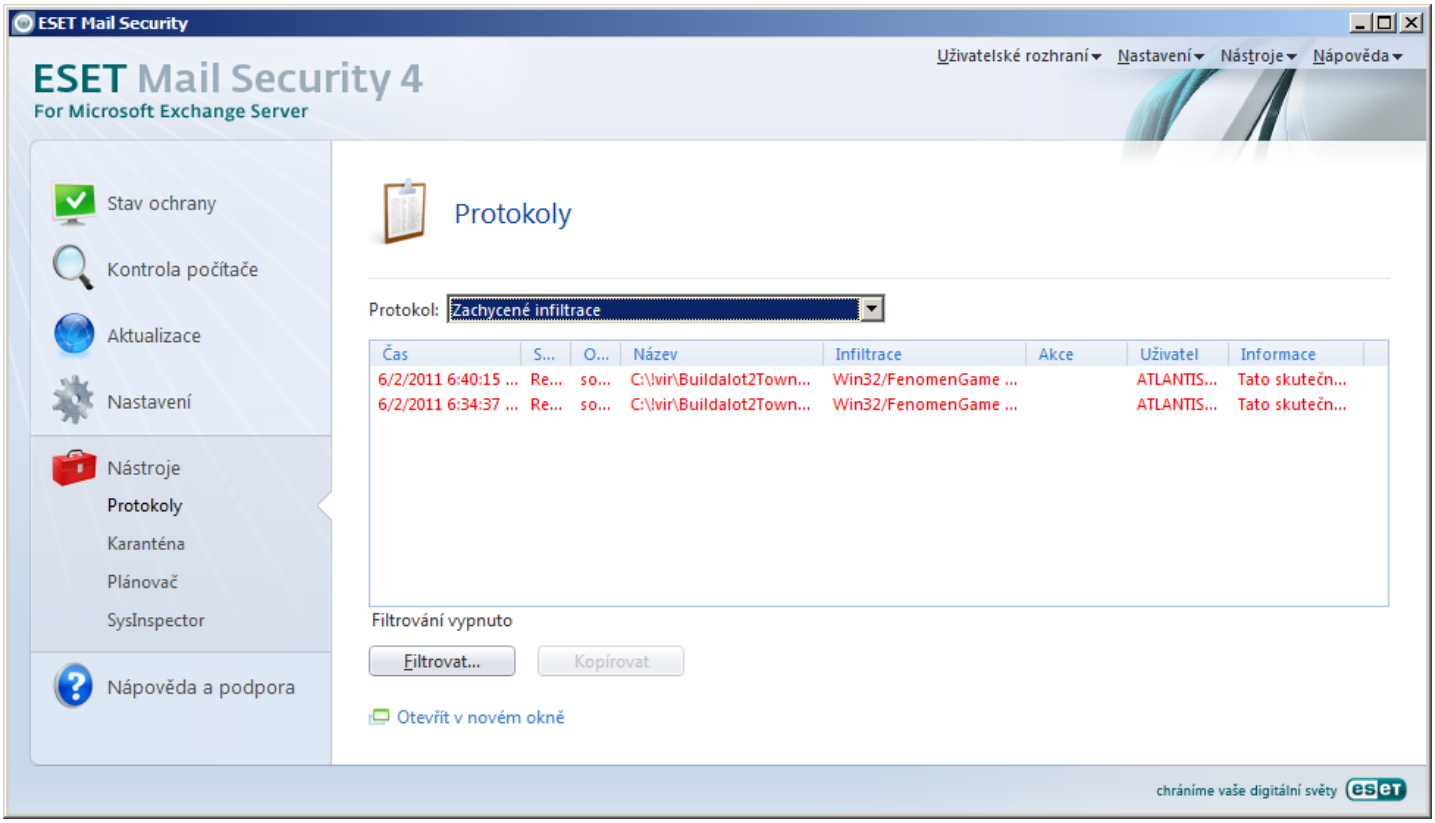
POZNÁMKA: Společnost ESET dostane denně tisíce souborů a není v jejich silách zasílat odpověď na každý poslaný soubor.



4.5 Protokoly

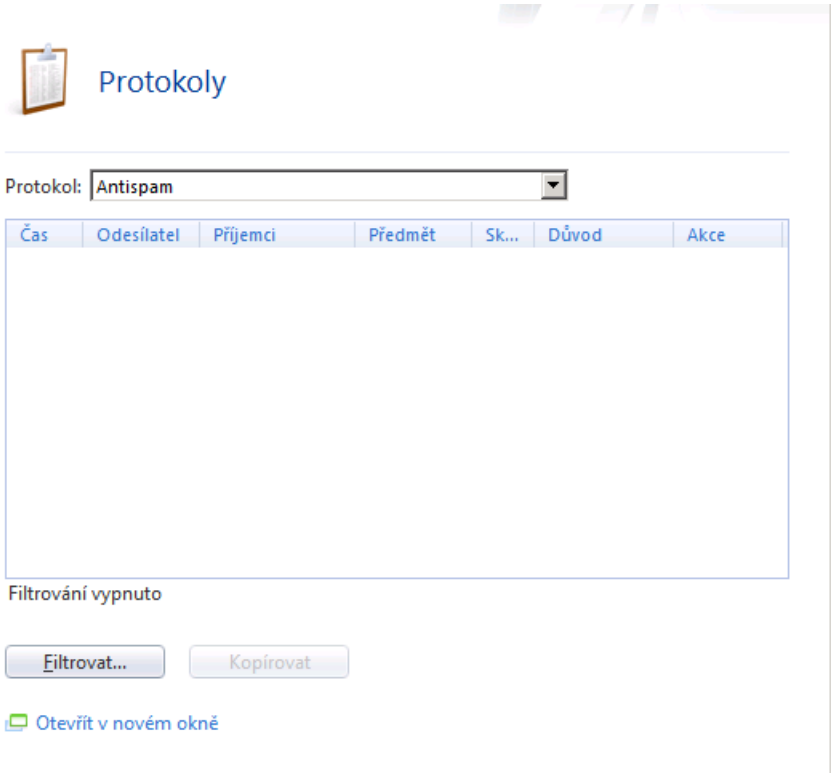
Protokoly uchovávají informace o důležitých událostech: zachycené infiltrace, záznamy z kontroly počítače, záznamy z rezidentní ochrany a systémových informacích.

Protokoly antispamové a greylistingovej ochrany (nacházejí se mezi ostatními protokoly v části **Nástroje> Protokoly**) podrobně zaznamenávají informace o zprávách, které prošly kontrolou včetně akcií, které s nimi byly provedeny. Mohou být velmi užitečné při hledání nedoručených mailů, pátrání po příčinách jejich označení jako spam a pod.



Antispam

Do tohoto protokolu se zaznamenávají všechny zprávy, které ESET Mail Security vyhodnotil jako spam, resp. jako pravděpodobný spam.



Význam jednotlivých sloupců:

Čas – čas, kdy byl přidán záznam do Antispam logu
Odesílatel – adresa odesílatele
Příjemce – adresa příjemce
Předmět – předmět zprávy
Skóre – spam skóre přidělené zpráve (v rozmezí od 0 do 100)
Důvod – indikátor, kvůli kterému byla zpráva vyhodnocena jako spam. Jde o indikátor s největší váhou. Pokud chcete znát i další ukazatele, dvojitým kliknutím na záznam otevřete okénko **Důvod** s dalšími detaily. Jednotlivé indikátory jsou seřazeny od hora směrem dolů, přičemž na nejvyšším místě se nachází indikátor s největší váhou a na posledním místě se nachází indikátor s nejnižší váhou.

URL Spammy Reputation	URL adresa ve zprávě se zvykne používat v spamových zprávách.
HTML Formatting (Fonts, colors, etc)	Formátování některých prvků v HTML části zprávy má vlastnosti charakteristické pro spam (typ a velikost fontu, jeho barva a pod.)
Spam Tricks: Obfuscation	Slova typická pro spam se snaží maskovat použitím jiných znaků. Typický příklad je slovo "Viagra", které se v spamových zprávách často zapisuje jako "V1agra" ve snaze vyhnout se detekci antispamem.
HTML Image Type spam	Ve snaze zakázat se některým antispamovým detekční metodám je spamový zpráva poslána jako obrázek, který je většinou i interaktivní linkou na nějakou webovou stránku.
URL formatting hosting service domain	URL adresa obsahuje doménu hostingové služby.
Spammy keyword ...	Zpráva obsahuje některá slova typické pro spam.
Email header inconsistency	Informace v záhlaví zprávy jsou změněna tak, aby zpráva působila dojmem, že pochází z jiného než skutečného zdroje.
Virus	Zpráva obsahuje podezřelou přílohu.
Phish	Zpráva obsahuje text typický pro emaily typu phishing.
Replica	Zpráva obsahuje text typický pro kategorii spamu, která se zabývá nabízením replik.
Generic spam indicator	Zpráva obsahuje některé typické slova / znaky charakteristické pro spam, jako např. "Dear friend", "hello winner", více vykřičníků za sebou "!!!" a pod.
Ham indicator	Tento indikátor má opačnou funkci než ostatní indikátory v tomto seznamu. Vyhodnocuje prvky, které jsou charakteristické pro řádnou

	(tedy ne spamovou) zprávu. Snižuje celkové spam skóre zprávy.
Non-specific spam indicator	Zpráva obsahuje jiné nespecifické spam prvky, např. base64 kódování.
Custom spam phrases	Různé jiné fráze typické pro spam.
URL is blacklisted	URL ve zprávě se nachází na blacklisty.
IP %s is on RBL	IP adresa ... se nachází na RBL seznamu.
URL %s is on DNSBL	URL adresa ... se nachází na DNSBL seznamu.
URL %s is on RBL or the server is not entitled to send mail	URL adresa ... se nachází na RBL seznamu nebo server nemá právo posílat emailové zprávy. Adresy, přes které přešel email se ověřují vůči RBL seznamu, přičemž u poslední adresy se zjišťuje i to zda má právo se připojovat se na veřejné mail servery. Jestliže toto právo nemá, nachází se na LBL seznamu. Zprávy označené jako spam kvůli záznamu v LBL seznamu mají jako důvod uvedeno "server is not entitled to send mail".

Akce – akce, která byla s zprávou provedena. Možné akce:

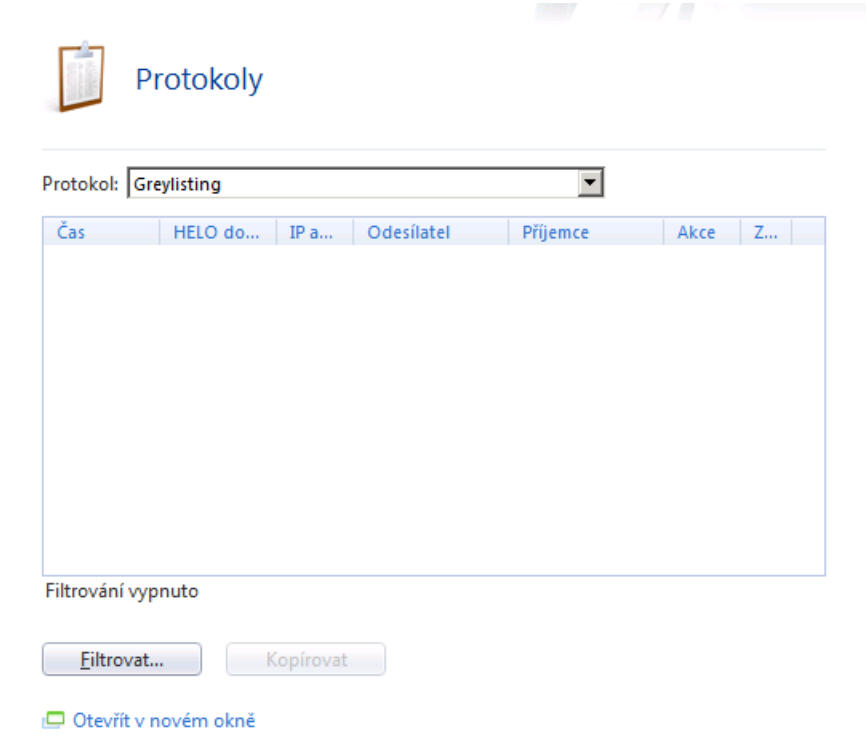
Retained	Se zprávou nebyla provedena žádná akce.
Quarantined	Zpráva byla uložena do karantény.
Cleaned and quarantined	Ze zprávy byl odstraněn virus a byla uložena do karantény.
Rejected	Zpráva byla zamítnuta a odesílateli byla zaslána SMTP reject odpověď 18.
Deleted	Zpráva byla zmazaná způsobem silent drop 18.

Přijaté – čas, kdy byla zpráva přijata na server.

Poznámka: V případě přijímání zpráv přes poštovní server jsou časy **Čas** a **Přijaté** prakticky stejné.

Greylisting

Do tohoto logu se zaznamenávají všechny zprávy, které byly nebo právě jsou vyhodnocovány metodou Greylisting.



Význam jednotlivých sloupců:

Čas – čas, kdy byl přidán záznam do Antispam logu
HELO doména – doménové jméno, kterým se identifikuje odesílající server vůči přijímacímu serveru
IP adresa – IP adresa odesílatele

Odesílatel – adresa odesílatele
Příjemce – adresa příjemce
Akce – může obsahovat tyto stavy:

Rejected	Příchozí zpráva byla podle zásady Greylisting zamítnuta (první pokus doručení)
Rejected (not verified)	Příchozí zpráva byla odesílajícím serverem opakovaně doručena, ale ještě neuběhl časový limit pro počáteční zamítnutí spojení (**Time limit for the initial connection denial**).
Verified	Příchozí zpráva byla odesílajícím serverem po opakovaných pokusech a uplynutí časového limitu **Time limit for the initial connection denial** úspěšně ověřena a doručena.

Zbývající čas – čas zbývající do uplynutí **Časového limitu pro počáteční zamítnutí spojení (v minutách):**

Zachycené infiltrace
Protokol zachycených infiltrací zobrazuje detailní informace o infiltracích zachycených moduly ESET Mail Security. Informace zahrnují čas zachycení, typ skeneru, druh objektu, název objektu, název infiltrace, místo, akce provedena a jméno uživatele přihlášeného v okamžiku zachycení infiltrace. Na kopírování, vymazání jedné nebo více řádků (nebo vyprázdnění celého protokolu), použijte kontextové menu (kliknutím pravého tlačítka na požadovanou položku).

Události
Protokol událostí obsahuje informace o událostech a chybách, které mohly nastat v programu. Často se tam dá najít informace, která vám pomůže odhalit případný problém, který se dá následně řešit.

Kontrola počítače
Protokol kontrola počítače uchovává informace o ručně spuštěných a plánovaných kontrol počítače. Každý řádek odpovídá jednotlivé kontroly počítače. Zobrazuje následující informace: čas kontroly, testovány adresáře, zkratku testovaných, infikovaných a vyléčených souborů spolu se současným stavem.

V protokolu **Kontrola počítače** máte možnost zobrazení detailního obsahu protokolu v odděleném okně pomocí poklepání na konkrétní záznam. Použijte kontextové menu (kliknutí pravým tlačítkem) na zkopírování jednoho, nebo více záznamů (funguje ve všech druzích protokolů).

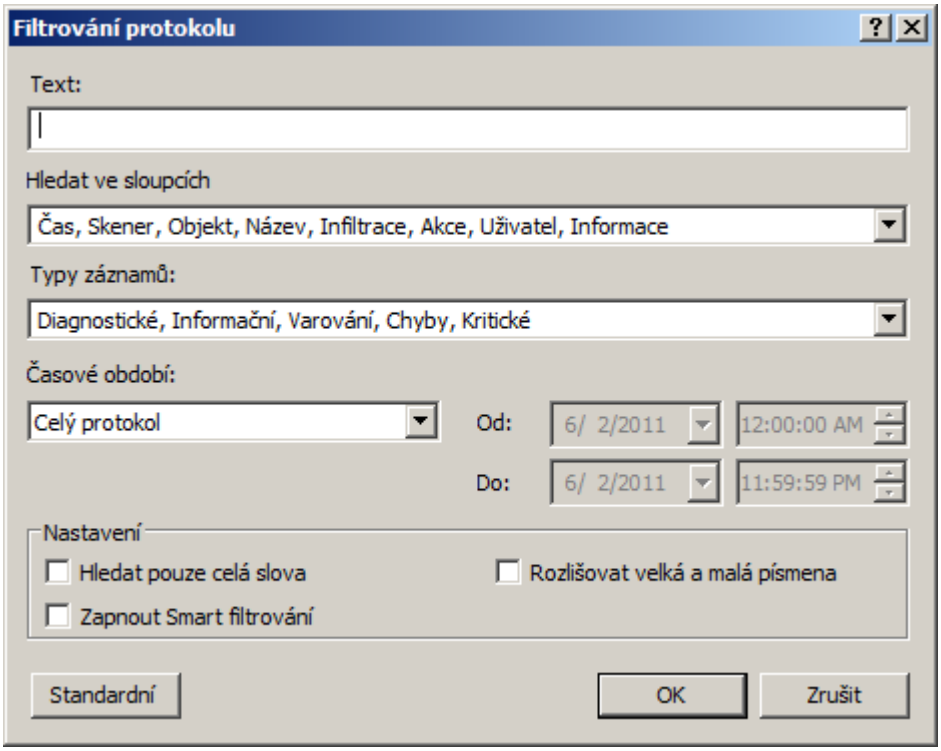
4.5.1 Filtrování protokolu

Protokoly je užitečný nástroj, který často pomůže vyhledat ve velkém množství záznamů potřebnou informaci.

Při použití funkce filtrování zadejte řetězec (**Text**), který filtrujete, zadejte sloupce ve kterých se má hledat (**Hledat ve sloupcích**), označte **Typy záznamů** a nastavte **Časové období.** Po vyspecifikován možností filtrování se zobrazí relevantní výsledky v okně **Protokoly**.

Okno **Filtrování protokolů** otevřete v menu volbou **Nástroje** > **Protokoly** a stisknutím tlačítka **Filtrovat...**, případně použitím zkratky Ctrl + Shift + F.

POZNÁMKA: Pro vyhledání konkrétního záznamu můžete použít funkci Nalézt v protokolu 84, případne ji využít ve spojení s funkcí **Filtrování protokolů**.



Po vyspecifikován možností filtrování se relevantní výsledky zobrazí v okně **Protokoly**. Takto vybraný seznam protokolů vám usnadní hledání konkrétního záznamu. Čím specifičtější kritéria použijete, tím konkrétnější bude konečný seznam zobrazených výsledků.

Text: - Vložte řetězec (slovo nebo část hledaného slova).

Hledat ve sloupcích: - Vyberte sloupce, které budou zohledněny při vyhledávání. Můžete označit jeden nebo více sloupců. Standardně jsou označeny všechny sloupce.

- **Čas**
- **Modul**
- **Událost**
- **Uživatel**

Typy záznamů: - Výběr typů záznamů, které se mají vyhledávat. Můžete vybrat jeden nebo více typů najednou. Standardně jsou označeny všechny typy záznamů.

- **Diagnostické**
- **Informační**
- **Varování**
- **Chyby**
- **Kritické**

Časové období: - Tuto možnost použijte, pokud chcete, aby byly vyhledávány pouze záznamy, které spadají do určeného časového období. Výběr obsahuje tyto možnosti:

- **Celý protokol**
- **Poslední den**
- **Poslední týden**
- **Poslední měsíc**
- **Časové období** – pomocí této možnosti můžete určit časový interval (datum a čas) pro zobrazení protokolů zaznamenaných v daném časovém období.

Kromě výše uvedených parametrů filtrování jsou vám k dispozici další **Nastavení**:

Hledat pouze celá slova – Zobrazí se pouze záznamy, které souhlasí s řetězcem zadaným v poli **Text**.
Rozlišovat velká a malá písmena – Zobrazí se pouze záznamy, které souhlasí včetně velkých a malých písmen s řetězcem zadaným v poli **Text**.
Zapnout Smart filtrování – Použijte tuto možnost, pokud chcete, aby ESET Mail Security použil vlastní metody filtrování.

Po nastavení možností filtrování stiskněte **OK** pro použití aktuálního filtru. Okno **Protokoly** zobrazí jen ty záznamy, které odpovídají nastaveným parametrům filtrování.

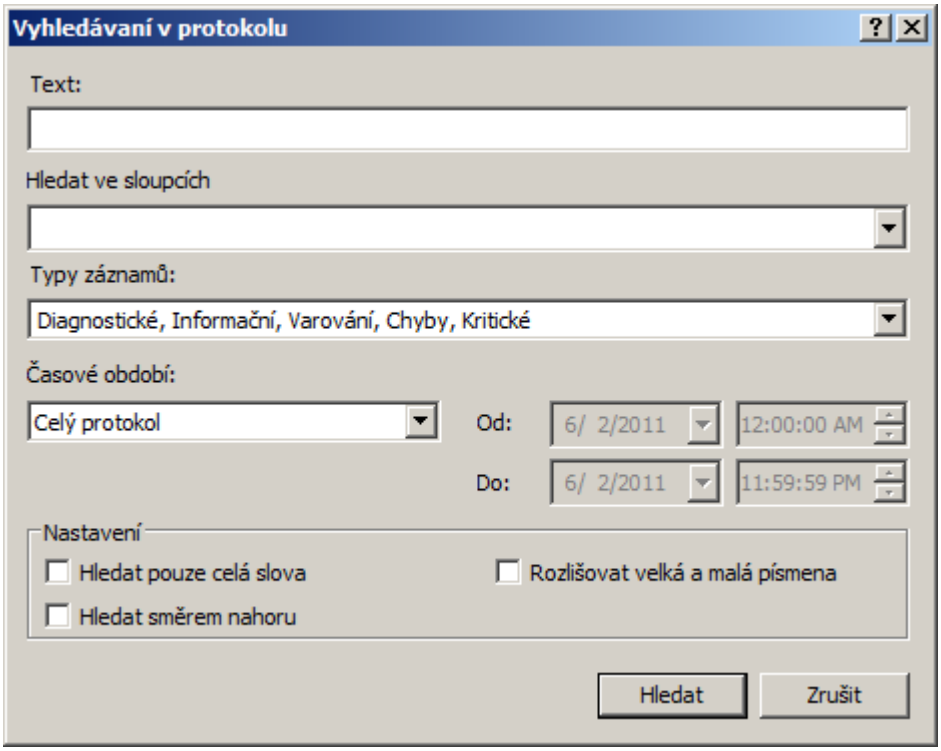
4.5.2 Vyhledávání v protokolu

Doplňkovou funkcí Filtrování protokolů 82 je vyhledávání v protokolech (vyhledávání však funguje i nezávisle a dá se použít i bez filtrování protokolů). Podobně jako při filtrování protokolů, vám vyhledávání umožní najít konkrétní informaci v protokolech. Hlavně v případě pokud protokolu velké množství záznamů.

Při použití funkce vyhledávaní v protokolu zadejte řetězec (**Text**), který hledáte, zadejte sloupce ve kterých se má hledat (**Hledat ve sloupcích**), označte **Typy záznamů** a nastavte **Časové období.**

Okno **Vyhledávaní v protokolu** otevřete pomocí použití zkratky Ctrl + f.

POZNÁMKA: Funkci Vyhledávaní v protokolu můžete použít spolu s funkcí Filtrování protokolu 82. Například můžete nejprve zúžit počet záznamů pomocí filtrování a následně začít vyhledávat.



Text: - Vložte řetězec (slovo nebo část hledaného slova).

Hledat ve sloupcích: - Vyberte sloupce, které budou zohledněny při vyhledávání. Můžete označit jeden nebo více sloupců. Standardně jsou označeny všechny sloupce.

- **Čas**
- **Modul**
- **Událost**
- **Uživatel**

Typy záznamů: - Výběr typů záznamů, které se mají vyhledávat. Můžete vybrat jeden nebo více typů najednou. Standardně jsou označeny všechny typy záznamů.

- **Diagnostické**
- **Informační**
- **Varování**
- **Chyby**
- **Kritické**

Časové období: - Tuto možnost použijte, pokud chcete, aby byly vyhledávány pouze záznamy, které spadají do určeného časového období. Výběr obsahuje tyto možnosti:

- **Celý protokol**
- **Poslední den**
- **Poslední týden**

- **Poslední měsíc**
- **Časové období** – pomocí této možnosti můžete určit časový interval (datum a čas) pro zobrazení protokolů zaznamenaných v daném časovém období.

Kromě výše uvedených parametrů vyhledávání jsou vám k dispozici další **Nastavení**:

Hledat pouze celá slova – Vyhledány budou pouze záznamy, které souhlasí s řetězcem zadaným v poli **Text**.
Rozlišovat velká a malá písmena – Vyhledány budou pouze záznamy, které souhlasí včetně velkých a malých písmen s řetězcem zadaným v poli **Text**.
Hledat směrem nahoru – Po zaškrtnutí se vyhledají záznamy směrem nahoru.

Po nastavení možností vyhledávání stiskněte tlačítko **Hledat**. Vyhledávání se zastaví při prvním nalezeném záznamu, který odpovídá parametrům vyhledávání. Opět klikněte na tlačítko **Hledat** pokud chcete pokračovat v hledání. Protokoly jsou prohledávány směrem shora dolů, počínaje z dané pozice (záznam, který je momentálně označen).

4.5.3 Správa protokolů

Nastavení možností protokolování produktu ESET Mail Security je možné přes hlavní okno programu > **Nastavení** >
Zobrazit celý strom pokročilých nastavení > **Nástroje** > **Protokoly**. Je možné definovat tyto vlastnosti protokolů:

- **Automaticky smazat záznamy protokolů**: po uplynutí zvoleného časového období jsou starší záznamy vymazány.

- **Automaticky optimalizovat protokoly**: umožňuje defragmentaci databáze podle nastavení limitního počtu nevyužitých záznamů.

- **Zaznamenávat události od úrovně**: určuje podrobnost protokolování. Lze nastavit následující úrovně:

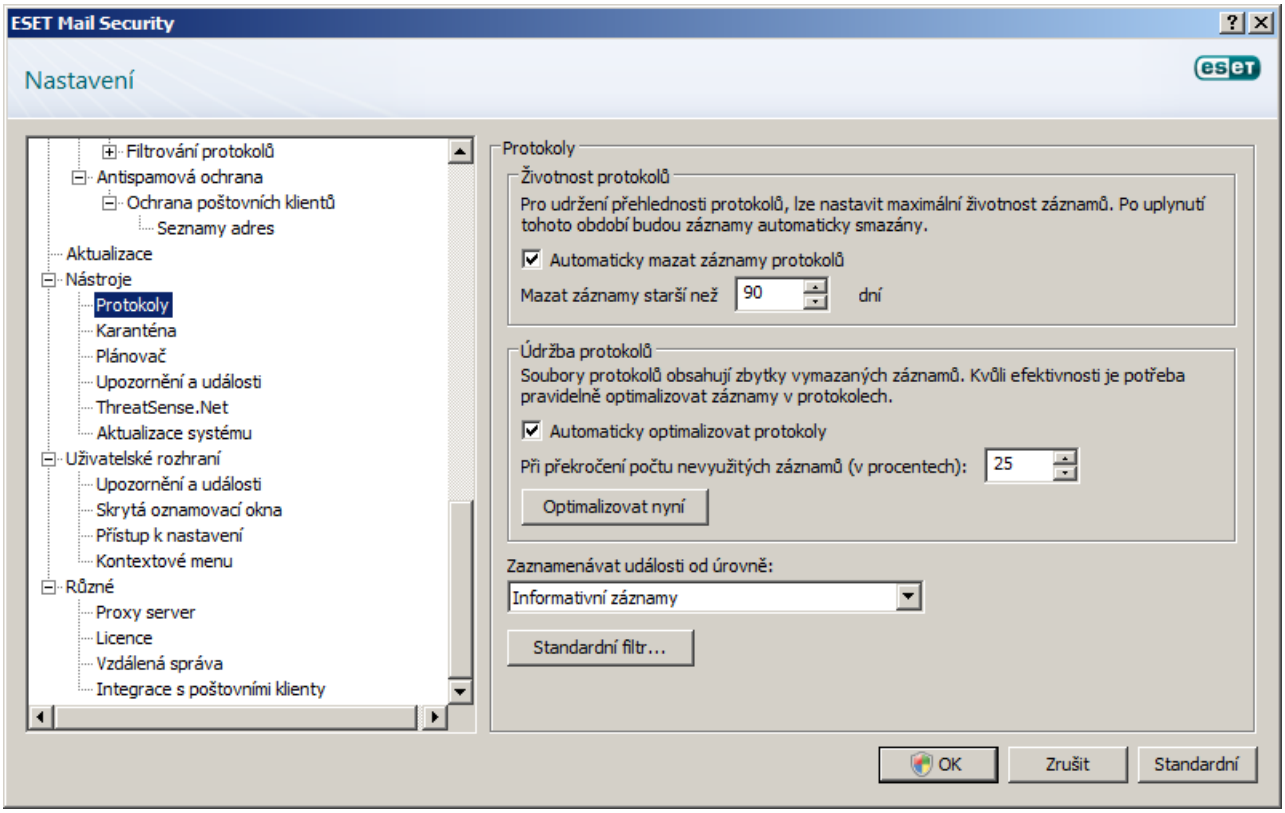
– **Kritické chyby** – zaznamenávány budou pouze kritické chyby (nespuštění antivirové ochrany, personálního firewallu apod.)

– **Chyby** – zaznamenávány boudou chyby typu „Chyba při stahování souboru aktualizace" a kritické chyby.

– **Varování** – zaznamenávány budou varovné zprávy, chyby a kritické chyby.

– **Informační záznamy** – zaznamenávány budou informační zprávy, například o úspěšné aktualizaci, a všechny výše uvedené záznamy.

– **Diagnostické záznamy** –zaznamenávány budou informace důležité pro ladění programu a všechny výše uvedené záznamy.



4.6 ESET SysInspector

4.6.1 Úvod do programu ESET SysInspector

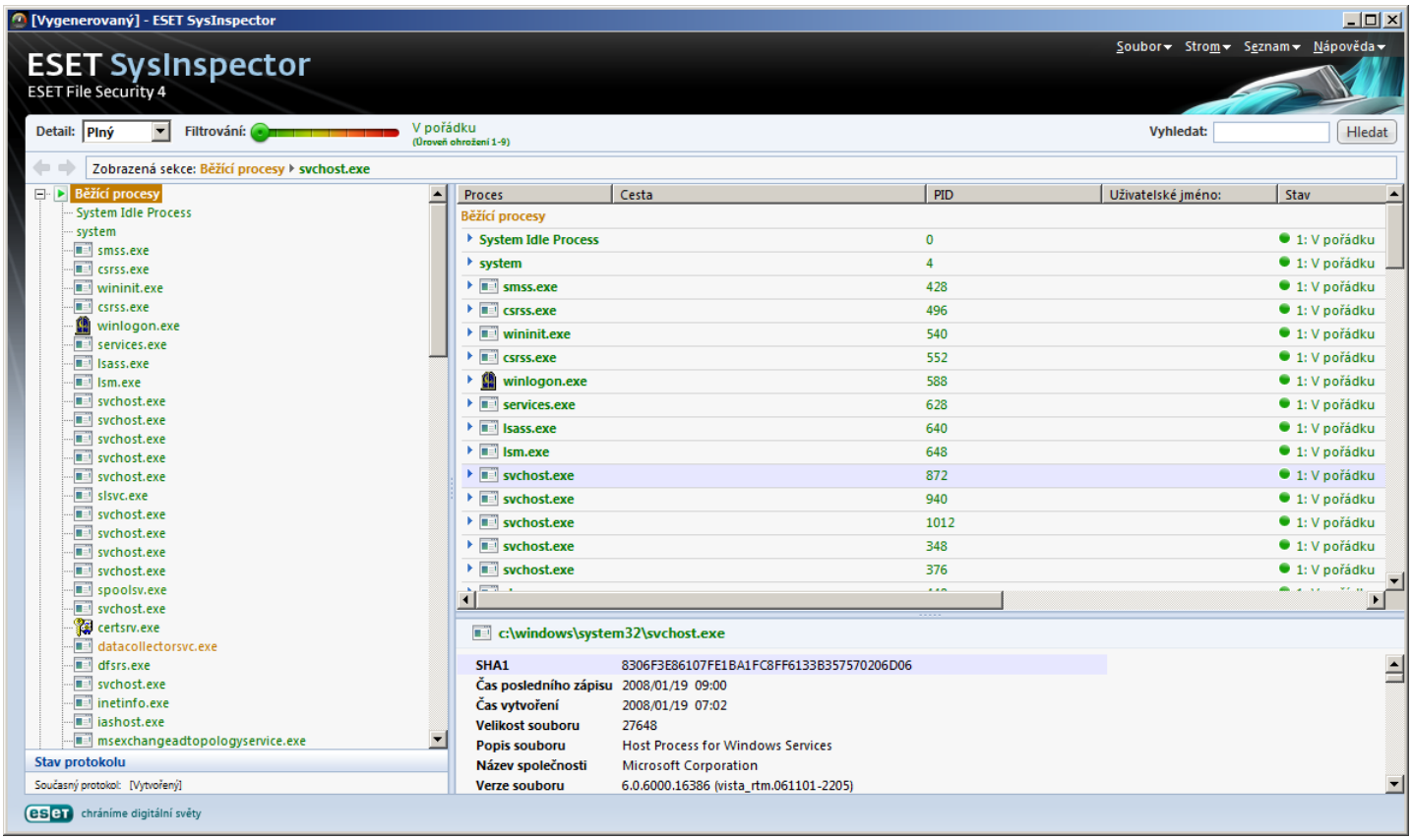
ESET SysInspector je aplikácia, ktorá dôkladne prehliadne váš počítač a zobrazí zozbierané dáta v súhrnnom náhľade. Informácie ako nainštalované ovládače a aplikácie, sieťové pripojenia, či dôležité položky registra Windows vám môžu pomôcť pri zisťovaní príčiny podozrivého správania sa systému, či už kvôli softwarovej alebo hardwarovej nekompatibilite alebo malwarovej infiltrácii.

4.6.1.1 Spustenie programu ESET SysInspector

Pre spustenie programu ESET SysInspector jednoducho spustite *SysInspector.exe*. Následne, prosím, počkajte, kým aplikácia prehliadne váš systém, čo môže trvať aj niekoľko minút v závislosti od vášho hardwaru a dát, ktoré sa majú zozbierať.

4.6.2 Užívateľské rozhranie a používanie aplikácie

Pre jednoduché používanie je hlavné okno rozdelené do štyroch hlavných sekcií – Ovládanie programu (1) je umiestnené hore v hlavnom okne, navigačné okno (3) je naľavo a okno s popisom (2) je napravo v strednej časti. Okno s detailmi (4) sa nachádza v pravej časti dole. Sekcia Stav protokolu (5) zobrazuje základné parametre protokolu (použitý filter, typ filtra, či je protokol výsledkom porovnania, atď.).



4.6.2.1 Ovládacie prvky programu

Táto sekcia obsahuje popis všetkých ovládacích prvkov dostupných v programe ESET SysInspector.

Súbor
Kliknutím sem si môžete uložiť váš súčasný protokol pre neskoršie preskúmanie, alebo otvoriť predtým uložený protokol. Ak chcete váš protokol zverejniť, odporúčame ho vygenerovať ako vhodný na posielanie. V tomto prípade sa vynechajú citlivé informácie.

Poznámka: Uložené protokoly programu ESET SysInspector môžete jednoducho otvoriť pretiahnutím súboru do hlavného okna.

Strom
Umožňuje vám rozbaliť alebo zatvoriť všetky vetvy a vyexportovať vybrané časti do Servisného skriptu.

Zoznam
Obsahuje funkcie pre jednoduchšiu navigáciu v programe a ďalšie funkcie, ako napríklad vyhľadávanie informácií online.

Pomoc
Obsahuje informácie o aplikácii a jej funkciách.

Detail
Ovplyvňuje informácie zobrazené v ostatných sekciách hlavného okna a tým robí používanie programu jednoduchým. V "Základnom" móde máte prístup k informáciám, ktoré sa používajú na nájdenie bežných problémov v systéme. V "Strednom" móde program zobrazuje aj menej používané detaily, zatiaľ čo v "Plnom" móde ESET SysInspector zobrazí všetky informácie potrebné k vyriešeniu veľmi špecifických problémov.

Filtrovanie
Sa používa najlepšie na vyhľadanie podozrivých súborov alebo zápisov v registri vo vašom systéme. Nastavením posuvníka môžete filtrovať položky podľa ich úrovne rizika. Ak je posuvník nastavený čo najviac vľavo (Filtrovanie 1), tak sú zobrazené všetky položky. Nastavením posuvníka viac doprava odfiltrujete všetky položky s úrovňou rizika menšou, než je aktuálne nastavená a zobrazíte viac podozrivé položky. Ak je posuvník nastavený čo najviac vpravo, program zobrazí iba známe škodlivé položky.

Všetky položky, ktoré majú úroveň rizika 6 až 9 môžu predstavovať bezpečnostné riziko. Ak nepoužívate niektoré bezpečnostné riešenie od spoločnosti ESET, odporúčame, aby ste si preskenovali váš systém pomocou ESET Online Scanner, ak ESET SysInspector našiel takúto položku. ESET Online Scanner je zadarmo dostupná služba.

Poznámka: Úroveň rizika niektorej položky sa dá rýchlo určiť porovnaním farby danej položky s farbou na posuvníku úrovne rizika.

Vyhľadaj
Vyhľadávanie sa dá použiť pre rýchle hľadanie špecifickej položky alebo časti jej mena. Výsledky požiadavky na hľadanie sú zobrazené v časti s popisom.

Návrat
Kliknutím na šípku späť alebo dopredu sa môžete vrátiť k predošlej zobrazenej informácii v okne s popisom. Namiesto klikania na šípky môžete použiť klávesy backspace a medzerník.

Zobrazená sekcia
Zobrazuje súčasnú vetvu v navigačnom okne.

Dôležité: Položky vyznačené červenou farbou sú neznáme, preto ich program označí ako potenciálne nebezpečné. Ak je niektorá položka v červenom, neznamená to, že môžete automaticky zmazať daný súbor. Pred samotným zmazaním sa uistite, že súbory sú skutočne nebezpečné alebo nepotrebné.

4.6.2.2 Navigácia v programe ESET SysInspector

ESET SysInspector rozdeľuje niekoľko typov informácií do niekoľkých základných sekcií, ktoré sa nazývajú uzly. Ak je dostupných viac informácií, môžete ich nájsť po rozbalení každého uzla, kde uvidíte jeho poduzly. Pre rozbalenie alebo zavretie uzla, dvakrát poklikajte na názov, alebo kliknite na ⊞ alebo ⊟ vedľa názvu uzla. Pri prehliadaní stromovej štruktúry uzlov a poduzlov v navigačnom okne, môžete nájsť viac detailov pre každý uzol v okne s popisom. Ak prehliadate položky v okne s popisom, ďalšie detaily pre každý typ položky môžu byť zobrazené v okne s detailmi.

Nasledujú popisy hlavných uzlov v navigačnom okne a súvisiace informácie v oknách s popisom a detailmi.

Bežiace procesy
Táto vetva obsahuje informácie o aplikáciách a procesoch, ktoré sú spustené v čase generovania protokolu. V okne s popisom môžete nájsť ďalšie detaily pre každý proces, ako napríklad ktoré dynamické knižnice proces používa a ich umiestnenie v systéme, meno dodávateľa aplikácie, úroveň rizika daného súboru, atď.

Okno s detailmi obsahuje ďalšie informácie pre položky vybrané v okne s popisom, ako napríklad veľkosť súboru alebo jeho kontrolný súčet.

Poznámka: Operačný systém pozostáva z niekoľkých dôležitých komponentov jadra systému, ktoré bežia nepretržite a poskytujú základnú a vitálnu funkcionalitu pre ostatné užívateľské aplikácie. V niektorých prípadoch sú takéto procesy zobrazené v protokole ESET SysInspector s cestou začínajúcou na \??\. Tieto symboly poskytujú optimalizáciu ešte pred spustením pre tieto procesy; sú bezpečné pre systém a ako také sú korektné.

Sieťové pripojenia
Okno s popisom obsahuje zoznam procesov a aplikácií, ktoré komunikujú cez sieť pomocou protokolu, ktorý je vybraný v navigačnom okne (TCP alebo UDP) a tiež aj vzdialenú adresu, kam sa daná aplikácia pripája. Taktiež môžete skontrolovať IP adresy DNS serverov.

Okno s detailmi obsahuje dodatočné informácie pre položky vybrané v okne s popisom, ako napríklad veľkosť súboru alebo jeho kontrolný súčet.

Dôležité záznamy registrov
Obsahuje zoznam vybraných položiek registra Windows, ktoré často súvisia s rôznymi problémami vo vašom počítači, napríklad tie, ktoré definujú programy spúšťané po štarte, browser helper objects (BHO), atď.

V okne s popisom môžete nájsť, ktoré súbory súvisia so špecifickými položkami v registri. Viac detailov môžete vidieť v okne s detailmi.

Služby
Okno s popisom obsahuje zoznam súborov, ktoré sú zaregistrované ako služby systému Windows. Môžete si skontrolovať, akým spôsobom sa služba spúšťa spoločne so špecifickými detailmi súboru v okne s detailmi.

Ovládače
Zoznam ovládačov, ktoré sú nainštalované v systéme.

Kritické súbory
Okno s popisom zobrazí obsah s kritickými súbormi súvisiacimi s operačným systémom Microsoft Windows.

Systémové informácie
Obsahuje detailné informácie o hardwari a softwari spoločne s informáciami o nastavených globálnych premenných a užívateľských právach.

Detaily súborov
Zoznam dôležitých systémových súborov a súborov v adresári Program Files. Ďalšie informácie, špecifické pre súbory, sa dajú nájsť v oknách s popisom a detailmi.

O programe
Informácie o programe ESET SysInspector.

4.6.2.3 Porovnanie protokolov

Funkcia Porovnanie protokolov umožňuje užívateľovi porovnať dva existujúce protokoly. Výstup z tejto funkcionality je sada položiek, ktoré nie sú spoločné pre obidva protokoly. Je to vhodné, ak chcete sledovať zmeny v systéme – môžete napríklad objaviť aktivitu škodlivého programu.

Po tom, čo je spustená, aplikácia vytvorí nový protokol, ktorý sa zobrazí v novom okne. Choďte do **Súbor > Ulož protokol** pre uloženie protokolu do súboru. Protokoly sa dajú otvoriť a prezerať aj neskôr. Pre otvorenie už existujúceho protokolu, použite menu **Súbore > Načítaj protokol**. V hlavnom okne programu ESET SysInspector sa vždy zobrazí naraz iba jeden protokol.

Ak porovnávate dva protokoly, princíp spočíva v tom, že porovnávate práve aktívny protokol s protokolom uloženým v súbore. Pre porovnanie protokolov použite voľbu **Súbor > Porovnanie protokolov** a zvoľte **Výber súboru**. Vybraný protokol bude porovnaný s aktívnym v hlavnom okne programu. Výsledný, tzv. zrovnávací protokol zobrazí iba rozdiely medzi tými dvomi protokolmi.

Poznámka: V prípade, že porovnávate dva protokoly, vyberiete voľbu **Súbor > Ulož protokol** a uložíte ich ako ZIP súbor, obidva súbory sú uložené. Ak neskôr otvoríte takýto súbor, protokoly, ktoré obsahuje, budú automaticky porovnané.

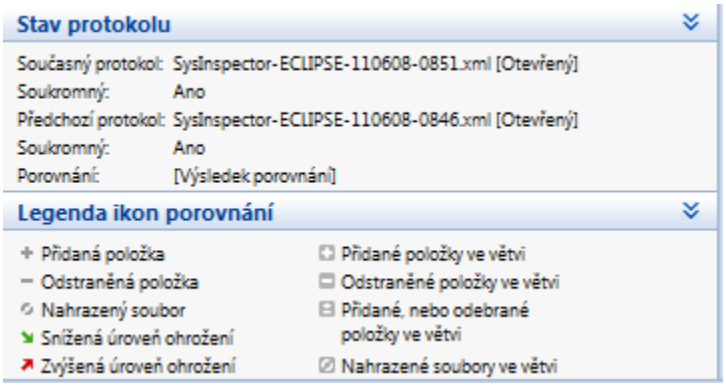
Vedľa zobrazených položiek, SysInspector zobrazí symboly identifikujúce rozdiely medzi porovnávanými protokolmi.
Položky označené ako – sa nachádzajú iba v aktívnom protokole a neboli prítomné v otvorenom zrovnávacom protokole. Položky označené ako +, na druhej strane, boli prítomné iba v otvorenom protokole a chýbajú v tom aktívnom.

Popis všetkých symbolov, ktoré môžu byť zobrazené vedľa symbolov:

+ nová hodnota, nebola prítomná v predchádzajúcom protokole
▫ sekcia so stromovou štruktúrou obsahuje nové hodnoty
– odobraná hodnota, prítomná iba v predchádzajúcom protokole
▪ sekcia so stromovou štruktúrou obsahuje odobrané hodnoty
⎋ hodnota / súbor boli zmenené

sekcia so stromovou štruktúrou obsahuje zmenené hodnoty / súbory
úroveň rizika poklesla / bola vyššia v predošlom protokole
úroveň rizika stúpla / bola nižšia v predošlom protokole

Vysvetľujúca sekcia zobrazená v ľavom dolnom rohu popisuje všetky symboly a tiež zobrazuje názvy protokolov, ktoré sú porovnávané.



Hociktorý zrovnávací protokol môže byť uložený do súboru a kedykoľvek neskôr otvorený.

Príklad:

Vygenerujte a uložte protokol, ktorý zaznamená originálne informácie o systéme do súboru *predchadzajuci.xml*. Po tom, čo budú vykonané zmeny v systéme, otvorte SysInspector a nechajte ho vygenerovať nový protokol. Uložte ho do súboru *aktualny.xml*.
Aby sme mohli sledovať zmeny medzi týmito dvomi protokolmi, choďte do menu **Súbor > Porovnanie protokolov**. Program vytvorí zrovnávací protokol, ktorý ukazuje rozdiely medzi protokolmi.

Rovnaký výsledok sa dá dosiahnuť, ak použijete nasledovnú voľbu v príkazovom riadku:

SysIsnpector.exe aktualny.xml predchadzajuci.xml

4.6.3 Ovládanie cez príkazový riadok

ESET SysInspector podporuje generovanie protokolov z príkazového riadku za použitia týchto parametrov:

/gen	vygeneruje protokol priamo z príkazového riadku bez spustenia grafického rozhrania
/privacy	vygeneruje protokol bez citlivých informácií
/zip	uloží výsledný protokol priamo na disk v komprimovanom súbore
/silent	tento parameter potlačí zobrazenie ukazateľa stavu pri generovaní protokolu
/help, **/?**	zobrazí informácie o použití parametrov v príkazovom riadku

Príklady

Pre zobrazenie niektorého protokolu priamo do prehliadača, použite: *SysInspector.exe "c:\klientskyprotokol.xml"*
Pre vygenerovanie protokolu do aktuálneho adresára, použite: *SysInspector.exe /gen*
Pre vygenerovanie protokolu do špecifického adresára, použite: *SysInspector.exe /gen="c:\adresar\"*
Pre vygenerovanie protokolu do špecifického súboru/lokácie, použite: *SysInspector.exe /gen="c:\adresar\mojnovyprotokol.xml"*
Pre vygenerovanie protokolu bez citlivých informácií, použite: *SysInspector.exe /gen="c:\mojnovyprotokol.zip" /privacy /zip*
Pre porovnanie dvoch protokolov, použite: *SysInspector.exe "aktualny.xml" "originalny.xml"*

Poznámka: Ak názov súboru/adresára obsahuje medzeru, mal by byť napísaný medzi úvodzovkami.

4.6.4 Servisný skript

Servisný skript je nástroj, ktorý slúži na poskytnutie pomoci zákazníkom, ktorí používajú ESET SysInspector. Slúži na odstránenie nežiaducich objektov zo systému.

Servisný skript umožňuje užívateľovi vyexportovať celý SysInspector protokol alebo iba vybrané časti. Po exporte môžete označiť nežiaduce objekty na zmazanie. Potom môžete spustiť modifikovaný protokol pre zmazanie označených objektov.

Servisný skript je vhodný pre pokročilých užívateľov s predošlými skúsenosťami v diagnostikovaní systémových problémov. Nekvalifikované zásahy môžu viesť k strate funkčnosti operačného systému.

Príklad:

Ak máte podozrenie, že je váš počítač napadnutý vírusom, ktorý nie je detegovaný vašim antivírusovým programom, pokračujte podľa nasledovných krokov:

- Spustite ESET SysInspector a vygenerujte nový protokol o systéme.
- Označte prvú položku v sekcii naľavo (v stromovej štruktúre), stlačte Ctrl a označte poslednú položku pre označenie všetkých položiek. Pustite Ctrl.
- Kliknite pravým tlačidlom myši na označené objekty a zvoľte **Ulož vybrané sekcie do servisného skriptu** z kontextového menu.
- Vybrané objekty budú vyexportované do nového protokolu.
- Toto je najdôležitejší krok v celej procedúre: otvorte nový protokol a zmeňte atribút – na + pre všetky objekty, ktoré chcete odstrániť. Prosím, uistite sa, že neoznačíte žiadne objekty, ktoré sú potrebné pre správne fungovanie systému.
- Otvorte ESET SysInspector, kliknite na **Súbor > Spusti servisný skript** a vložte cestu k vášmu skriptu.
- Kliknite na **OK** pre spustenie skriptu.

4.6.4.1 Generovanie servisného skriptu

Pre vygenerovanie skriptu, kliknite pravým tlačidlom myši na ľubovoľnú položku v stromovej štruktúre (v ľavej časti) v hlavnom okne programu SysInspector. Z kontextového menu vyberte buď voľbu **Ulož všetky sekcie do servisného skriptu** alebo **Ulož vybrané sekcie do servisného skriptu**.

Poznámka: Nie je možné vyexportovať servisný skript, keď sa porovnávajú dva protokoly.

4.6.4.2 Štruktúra servisného skriptu

V prvom riadku hlavičky skriptu sa nachádzajú informácie o verzii enginu (ev), verzii grafického rozhrania (gv) a verzii protokolu (lv). Tieto dáta môžete použiť pri hľadaní možných zmien v .xml súbore, ktorý generuje skript a zamedziť všetkým nezrovnalostiam počas vykonania skriptu. Táto časť skriptu by nemala byť modifikovaná.

Zvyšok súboru je rozdelený do sekcií, v ktorých sa môžu jednotlivé položky modifikovať (označiť tie, ktoré budú spracované skriptom). Položky označíte na spracovanie tak, že zameníte znak "-" pred položkou za znak "+". Jednotlivé sekcie v skripte sú oddelené prázdnym riadkom. Každá sekcia ma číslo a nadpis.

01) Running processes

Táto sekcia obsahuje zoznam všetkých bežiacich procesov v systéme. Každý proces je identifikovaný svojou UNC cestou a následne aj kontrolným súčtom CRC16 medzi hviezdičkami (*).

Príklad:

```
01) Running processes:
- \SystemRoot\System32\smss.exe *4725*
- C:\Windows\system32\svchost.exe *FD08*
+ C:\Windows\system32\module32.exe *CF8A*
[...]
```

V tomto príklade bol vybraný proces module32.exe (označený znakom "+"); proces bude ukončený pri spustení skriptu.

02) Loaded modules

Táto sekcia obsahuje zoznam aktuálne použitých systémových modulov.

Príklad:

```
02) Loaded modules:
- c:\windows\system32\svchost.exe
- c:\windows\system32\kernel32.dll
+ c:\windows\system32\khbekhb.dll
- c:\windows\system32\advapi32.dll
[...]
```

V tomto príklade bol modul khbekhb.dll bol označený znakom "+". Keď sa skript spustí, rozpozná procesy, ktoré používajú tento špecifický modul a ukončí ich.

O3) TCP connections

Táto sekcia obsahuje informácie o existujúcich TCP spojeniach.

Príklad:

```
03) TCP connections:
- Active connection: 127.0.0.1:30606 -> 127.0.0.1:55320, owner: ekrn.exe
- Active connection: 127.0.0.1:50007 -> 127.0.0.1:50006,
- Active connection: 127.0.0.1:55320 -> 127.0.0.1:30606, owner: OUTLOOK.EXE
- Listening on *, port 135 (epmap), owner: svchost.exe
+ Listening on *, port 2401, owner: fservice.exe Listening on *, port 445 (microsoft-ds), owner: System
[...]
```

Keď sa skript spustí, nájde vlastníka socketu v označených TCP spojeniach a zastaví tento socket, čím uvoľní systémové prostriedky.

O4) UDP endpoints

Táto sekcia obsahuje informácie o existujúcich koncových bodoch UDP.

Príklad:

```
04) UDP endpoints:
- 0.0.0.0, port 123 (ntp)
+ 0.0.0.0, port 3702
- 0.0.0.0, port 4500 (ipsec-msft)
- 0.0.0.0, port 500 (isakmp)
[...]
```

Keď sa skript spustí, izoluje vlastníka socketu v označených koncových bodoch UDP a zastaví tento socket.

O5) DNS server entries

Táto sekcia obsahuje informácie o súčasnej konfigurácií DNS serverov.

Príklad:

```
05) DNS server entries:
+ 204.74.105.85
- 172.16.152.2
[...]
```

Označené záznamy DNS budú odstránené, keď spustíte skript.

O6) Important registry entries

Táto sekcia obsahuje informácie o dôležitých záznamoch v registri Windows.

Príklad:

```
06) Important registry entries:
* Category: Standard Autostart (3 items)
 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HotKeysCmds = C:\Windows\system32\hkcmd.exe
```

```
- IgfxTray = C:\Windows\system32\igfxtray.exe
 HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Google Update = "C:\Users\antoniak\AppData\Local\Google\Update\GoogleUpdate.exe" /c
* Category: Internet Explorer (7 items)
 HKLM\Software\Microsoft\Internet Explorer\Main
+ Default_Page_URL = http://thatcrack.com/
[...]
```

Označené hodnoty budú zmazané, redukované na 0 bytové hodnoty, alebo vynulované do základných hodnôt po spustení skriptu. Akcia, ktorá sa vykoná po spustení skriptu, závisí od kategórie danej položky a kľúčovej hodnoty v špecifickej vetve v registri.

07) Services

Táto sekcia obsahuje zoznam služieb, ktoré sú zaregistrované v systéme.

Príklad:

```
07) Services:
- Name: Andrea ADI Filters Service, exe path: c:\windows\system32\aeadisrv.exe, state: Running, startup: Automatic
- Name: Application Experience Service, exe path: c:\windows\system32\aelupsvc.dll, state: Running, startup: Automatic
- Name: Application Layer Gateway Service, exe path: c:\windows\system32\alg.exe, state: Stopped, startup: Manual
[...]
```

Služby, ktoré sú označené a tiež služby, ktoré sú na nich závislé, budú po spustení skriptu zastavené a odinštalované.

08) Drivers

Táto sekcia obsahuje zoznam nainštalovaných ovládačov.

Príklad:

```
08) Drivers:
- Name: Microsoft ACPI Driver, exe path: c:\windows\system32\drivers\acpi.sys, state: Running, startup: Boot
- Name: ADI UAA Function Driver for High Definition Audio Service, exe path: c:\windows\system32\drivers\adihdaud.sys,
[...]
```

Keď spustíte skript, zvolené ovládače budú odregistrované zo systému a následne odstránené.

09) Critical files

Táto sekcia obsahuje informácie o súboroch, ktoré sú kritické pre správne fungovanie operačného systému.

Príklad:

```
09) Critical files:
* File: win.ini
- [fonts]
- [extensions]
- [files]
- MAPI=1
[…]
* File: system.ini
- [386Enh]
- woafont=dosapp.fon
- EGA80WOA.FON=EGA80WOA.FON
[…]
* File: hosts
- 127.0.0.1 localhost
- ::1 localhost
[…]
```

Zvolené položky budú buď odstránené, alebo vynulované do ich pôvodných hodnôt.

4.6.4.3 Spúšťanie servisných skriptov

Označte všetky požadované položky, potom skript uložte a zavrite. Spustite pozmenený skript priamo z hlavného okna programu SysInspector zvolením možnosti Spusti servisný skript z menu Súbor. Keď otvoríte skript, program vám zobrazí nasledovnú hlášku: **Ste si istý vykonaním servisného skriptu "%Scriptname%"?** Po tom, čo potvrdíte váš výber, môže sa objaviť ďalšie upozornenie, ktoré vás informuje, že servisný skript, ktorý sa pokúšate spustiť, nebol podpísaný. Kliknite na **Run** pre spustenie skriptu.

Dialógové okno potvrdí úspešné vykonanie skriptu.

Ak mohol byť skript spracovaný iba z časti, objaví sa dialógové okno s nasledovnou správou: **The service script was run partially. Do you want to view the error report?** Zvoľte **Yes** pre zobrazenie komplexného chybového protokolu, v ktorom bude zoznam operácií, ktoré sa nevykonali.

Ak nebol skript rozpoznaný, objaví sa dialógové okno s nasledovnou správou: **The selected service script is not signed. Running unsigned and unknown scripts may seriously harm your computer data. Are you sure you want to run the script and carry out the actions?** Toto môže byť spôsobené nezrovnalosťami v skripte (poškodená hlavička, poškodený nadpis sekcie, chýbajúci prázdny riadok medzi dvomi sekciami, atď.). Môžete buď opätovne otvoriť servisný skript a napraviť chyby v ňom, alebo vytvoriť nový servisný skript.

4.6.5 Klávesové skratky

Klávesové skratky, ktoré sa dajú použiť pri práci s programom ESET SysInspector, zahŕňajú:

Súbor

Ctrl+O	otvorí existujúci protokol
Ctrl+S	uloží vytvorený protokol

Generovanie

Ctrl+G	štandardná kontrola stavu systému
Ctrl+H	urobí kontrolu systému, ktorá môže zaznamenať aj citlivé informácie (aktuálne užívateľské meno, názov počítača, názov domény, právomoci aktuálneho užívateľa, globálne premenné a všetky IP adresy sú preložené do doménových názvov) a tiež sú všetky adresy preložené do doménových názvov

Filtrovanie

1, O	bezpečné, sú zobrazené položky s úrovňou rizika 1-9
2	bezpečné, sú zobrazené položky s úrovňou rizika 2-9
3	bezpečné, sú zobrazené položky s úrovňou rizika 3-9
4, U	neznáme, sú zobrazené položky s úrovňou rizika 4-9
5	neznáme, sú zobrazené položky s úrovňou rizika 5-9
6	neznáme, sú zobrazené položky s úrovňou rizika 6-9
7, B	riskantné, sú zobrazené položky s úrovňou rizika 7-9
8	riskantné, sú zobrazené položky s úrovňou rizika 8-9
9	riskantné, sú zobrazené položky s úrovňou rizika 9
-	zníži úroveň rizika
+	zvýši úroveň rizika
Ctrl+9	mód filtrovania, rovnaká úroveň alebo vyššia
Ctrl+O	mód filtrovania, iba rovnaká úroveň

Zobrazenie

Ctrl+5	zobraziť podľa výrobcu, všetci výrobcovia
Ctrl+6	zobraziť podľa výrobcu, iba Microsoft
Ctrl+7	zobraziť podľa výrobcu, všetci ostatní výrobcovia
Ctrl+3	zobrazí plné detaily
Ctrl+2	zobrazí stredné detaily
Ctrl+1	základné zobrazenie
Backspace	urobí krok naspäť
Medzerník	urobí krok dopredu
Ctrl+W	rozbalí stromovú štruktúru
Ctrl+Q	zbalí stromovú štruktúru

Iné klávesové skratky

Ctrl+T	prejde na pôvodnú lokáciu položky po jej vybratí vo výsledkoch vyhľadávania
Ctrl+P	zobrazí základné informácie o položke
Ctrl+A	zobrazí plné informácie o položke
Ctrl+C	skopíruje stromovú vetvu aktuálnej položky
Ctrl+X	skopíruje všetky položky
Ctrl+B	vyhľadá informácie o označenej položke na internete
Ctrl+L	otvorí adresár, kde sa nachádza zvolený súbor
Ctrl+R	otvorí príslušnú položku v editore registrov
Ctrl+Z	skopíruje cestu k súboru (ak označená položka súvisí so súborom)
Ctrl+F	prepne sa do vyhľadávacieho políčka
Ctrl+D	zatvorí výsledky vyhľadávania
Ctrl+E	spustí servisný skript

Porovnávanie

Ctrl+Alt+O	otvorí pôvodný / zrovnávací protokol
Ctrl+Alt+R	zruší porovnanie
Ctrl+Alt+1	zobrazí všetky položky
Ctrl+Alt+2	zobrazí iba pridané položky, protokol zobrazí položky, ktoré sú prítomné v aktuálnom protokole
Ctrl+Alt+3	zobrazí iba odobraté položky, protokol zobrazí položky, ktoré sú prítomné v predchádzajúcom protokole
Ctrl+Alt+4	zobrazí iba nahradené položky (vrátane súborov)
Ctrl+Alt+5	zobrazí iba rozdiely medzi protokolmi
Ctrl+Alt+C	zobrazí porovnanie
Ctrl+Alt+N	otvorí aktuálny protokol
Ctrl+Alt+P	otvorí predošlý protokol

Rôzne

F1	zobrazí nápovedu
Alt+F4	zatvorí program
ALT+SHIFT+F4	zatvorí program bez opýtania
Ctrl+I	štatistiky protokolu

4.6.6 Systémové požiadavky

Pre hladkú prevádzku programu ESET SysInspector by systém mal spĺňať nasledovné hardwarové a softwarové požiadavky:

Windows 2000, XP, 2003
400 MHz 32-bit (x86) / 64-bit (x64)
128 MB RAM systémovej pamäte
10 MB voľného miesta
Super VGA (800 x 600)

Windows 7, Vista, 2008
1 GHz 32-bit (x86) / 64-bit (x64)
512 MB RAM systémovej pamäte
10 MB voľného miesta
Super VGA (800 x 600)

4.6.7 Často kladené otázky

Potrebuje ESET SysInspector práva Administrátora, aby fungoval korektne ?

Zatiaľ čo ESET SysInspector nepotrebuje práva Administrátora, aby sa spustil, niektoré informácie, ktoré zbiera, sú prístupné iba administrátorskému účtu. Spustenie programu ako Standard User alebo Restricted User bude mať za následok, že zozbiera menej informácií o operačnom prostredí.

Vytvorí ESET SysInspector súbor s protokolom ?

ESET SysInspector dokáže vytvoriť súbor s protokolom o konfigurácií vášho počítača. Pre uloženie súboru, zvoľte Súbor > Ulož protokol z hlavného menu. Protokoly sú uložené v XML formáte. Štandardne sa súbory ukladajú do adresára %USERPROFILE%\My Documents\ s názvom súboru podľa konvencie "SysInpsector-%COMPUTERNAME %-YYMMDD-HHMM.XML". Umiestnenie a názov protokolu môžete zmeniť pred uložením, ak si to želáte.

Ako si prezriem ESET SysInspector protokol ?

Pre zobrazenie protokolu, ktorý vytvoril ESET SysInspector, spustite program a zvoľte Súbor > Načítaj protokol z hlavného menu. Tiež môžete pretiahnuť súbor s protokolom priamo na ESET SysInspector aplikáciu. Ak si potrebujete často prezerať protokoly programu ESET SysInspector, odporúčame urobiť zástupcu súboru SYSINSPECTOR.EXE na vašu Plochu; potom môžete súbory s protokolmi priamo presúvať na uvedeného zástupcu pre prehliadanie. Z bezpečnostných dôvodov nemusí Windows Vista/7 povoliť preťahovanie súboru medzi oknami, ktoré majú rozdielne bezpečnostné práva.

Je k dispozícií špecifikácia formátu súboru s protokolom? Čo SDK ?

V súčasnosti nie je k dispozícií ani špecifikácia, ani SDK, keďže program je ešte stále vo vývoji. Po tom, čo bude program uvoľnený, môžeme tieto veci poskytnúť vzhľadom na spätnú odozvu užívateľov a ich požiadaviek.

Ako ESET SysInspector vyhodnotí riziko, ktoré predstavuje konkrétny objekt ?

Väčšinou ESET SysInspector priradí úroveň rizika objektom (súbory, procesy, kľúče v registri, atď.) použitím série heuristických pravidiel, ktoré skontrolujú charakteristiku každého objektu, a potom zváži potenciál pre škodlivú činnosť. Na základe týchto heuristík sa objektom priradí úroveň rizika od "1 - V poriadku (zelená)" do "9 - Nebezpečné (červená)." V ľavom navigačnom okne sú jednotlivé sekcie zafarbené farbou podľa objektu s najvyššou úrovňou rizika, ktorý sa v nich nachádza.

Znamená úroveň rizika "6 - Neznáme (červená)", že je objekt nebezpečný ?

Odhad programu ESET SysInspector nezaručuje, že je objekt škodlivý—toto rozhodnutie by mal urobiť bezpečnostný expert. Na čo je ESET SysInspector navrhnutý, je poskytnutie rýchleho odhadu bezpečnostnému expertovi, takže ten vie, na ktoré objekty v systéme sa má zamerať pre podrobnejšie preskúmanie neobvyklého chovania.

Prečo sa ESET SysInspector pripája na internet pri spustení ?

Ako mnohé iné aplikácie, aj ESET SysInspector je podpísaný digitálnym certifikátom, aby bolo možné zaručiť, že software bol vydaný spoločnosťou ESET a nebol modifikovaný. Aby sa mohol overiť daný certifikát, operačný systém kontaktuje certifikačnú autoritu pre overenie identity vydavateľa softwaru. Toto je normálne správanie pre všetky digitálne podpísané programy pod operačným systémom Microsoft Windows.

Čo je technológia Anti-Stealth ?

Technológia Anti-Stealth poskytuje efektívnu detekciu rootkitov.
Ak je systém napadnutý škodlivým kódom, ktorý sa správa ako rootkit, užívateľ je vystavený riziku poškodenia, straty alebo ukradnutia dát. Bez špeciálnych anti-rootkitovských nástrojov je takmer nemožné detegovať rootkity.

Prečo sú niekedy súbory označené ako "Podpísal Microsoft" a zároveň majú iné "Meno spoločnosti" ?

Pri pokuse identifikovať digitálny podpis spustiteľného súboru, SysInspector najskôr hľadá digitálny podpis vložený v súbore. Ak ho nájde, pre validáciu sa použije táto identifikácia. Na druhej strane, ak súbor neobsahuje digitálny

podpis, ESI začne hľadať príslušný CAT súbor (Security Catalog - %systemroot%\system32\catroot), ktorý obsahuje informácie o spracovávanom spustiteľnom súbore. V prípade, že sa nájde patričný CAT súbor, digitálny podpis toho CAT súboru sa použije pri overovacom procese spustiteľného súboru.

Toto je dôvod, prečo sú niekedy súbory označené ako "Podpísal Microsoft", ale majú iné "Meno spoločnosti".

Príklad:

Windows 2000 obsahuje aplikáciu HyperTerminal umiestnenú v *C:\Program Files\Windows NT*. Hlavný spustiteľný súbor aplikácie nie je digitálne podpísaný, ale SysInspector súbor označí ako podpísaný spoločnosťou Microsoft. Dôvodom je referencia v *C:\WINNT\system32\CatRoot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\sp4.cat* poukazujúca na *C:\Program Files\Windows NT\hypertrm.exe* (hlavný spustiteľný súbor aplikácie HyperTerminal) a *sp4.cat* je digitálne podpísaný spoločnosťou Microsoft.

4.7 ESET SysRescue

ESET SysRescue je utilita, ktorá umožňuje vytvoriť bootovateľný disk obsahujúci ESET NOD32 Antivirus (ENA), resp. ESET Smart Security (ESS). Hlavnou výhodou tohto nástroja je, že ENA/ESS tu beží nezávisle od aktuálne nainštalovaného operačného systému, pričom má priamy prístup k disku a celému súborovému systému. Takto je možné napríklad odstrániť z disku vírusy, ktoré nebolo možné zmazať štandardným spôsobom pri spustenom operačnom systéme a pod.

4.7.1 Minimálne požiadavky

ESET SysRescue pracuje v prostredí Microsoft Windows Preinstallation Environment (Windows PE) rady 2.x, ktoré je založené na Windows Vista. Windows PE je súčasťou voľne stiahnuteľného balíčka Windows Automated Installation Kit (Windows AIK), preto prítomnosť Windows AIK je jednou z podmienok pre úspešné vytvorenie ESET SysRescue (http://go.eset.eu/AIK).Vzhľadom na to, že podporovaný je iba 32-bitový Windows PE, je potrebné použiť 32-bitový inštalačný súbor ESS alebo ENA pri vytváraní ESET SysRescue na 64-bitových systémoch. ESET SysRescue podporuje Windows AIK verzie 1.1 a vyššie. ESET SysRescue je dostupné na produktoch ESS/EAV 4.0 a vyššie.
Podporované operačné systémy:

- Windows 7
- Windows Vista
- Windows Vista Service Pack 1
- Windows Vista Service Pack 2
- Windows Server 2008
- Windows Server 2003 Service Pack 1 s KB926044
- Windows Server 2003 Service Pack 2
- Windows XP Service Pack 2 s KB926044
- Windows XP Service Pack 3

4.7.2 Popis vytvorenia CD

Ak sú splnené minimálne požiadavky na vytvorenie ESET SysRescue CD, je to pomerne jednoduchá úloha. Pre spustenie sprievodcu ESET SysRescue kliknite na **Štart > Programy > ESET > ESET NOD32 Antivirus (alebo ESET Smart Security) > ESET SysRescue**.
Na začiatku je zisťovaná prítomnosť Windows AIK a vhodných zariadení na vytvorenie bootovateľného média. V ďalšom kroku si vyberiete cieľové médium, na ktorom bude ESET SysRescue umiestnené. Okrem fyzických zariadení (CD/DVD, USB) je možné ESET SysRescue uložiť aj do ISO súboru, ktorý je možné neskôr napáliť na CD/DVD, alebo použiť iným spôsobom (napr. vo virtuálnom prostredí - VMware, VirtualBox a pod.).
Po zadaní všetkých potrebných údajov sa v poslednom kroku zobrazia parametre kompilácie. Tieto je možné ešte pred jej spustením zmeniť. Podrobnejšie k jednotlivým položkám:
Adresáre 98
ESET Antivírus 98
Pokročilé 98
Zavádzacie USB zariadenie 98
Napaľovanie 98

4.7.2.1 Adresáre

Dočasný adresár je pracovný adresár, kde sa dočasne ukladajú súbory počas kompilácie ESET SysRescue.
ISO adresár je adresár, kde sa po skončení kompilácie uloží výsledný ISO súbor.
V tabuľke je zoznam všetkých lokálnych a sieťových namapovaných diskov spolu s veľkosťou voľného miesta, ktoré obsahujú. Pokiaľ je niektorý z adresárov umiestnený na disku, kde je priestoru príliš málo, je vhodné tento adresár premiestniť na disk s väčším množstvom voľného miesta. V opačnom prípade môže kompilácia predčasne skončiť v dôsledku nedostatku miesta na disku.

4.7.2.2 ESET Antivírus

Pre vytvorenie ESET SysRescue CD môže kompilátor použiť dva zdroje súborov ESET:
ESS/EAV adresár – v tomto prípade sa použijú súbory aktuálne nainštalovaného ESET produktu na danom počítači
MSI súbor – použijú sa súbory priamo z inštalačného MSI balíka

K dispozícii sú dva možné zdroje používateľského mena a hesla určeného pre aktualizáciu:
Nainštalované ESS/EAV – meno a heslo pre aktualizáciu sa prevezme z aktuálne nainštalovaného ESET Mail Security
Od používateľa – použije sa meno a heslo zadané v príslušných kolónkach

Poznámka: Aktualizácia ESET Smart Security respektíve ESET NOD32 Antivirusu nachádzajúceho sa na ESET SysRescue CD sa vykoná buď z internetu, alebo z bezpečnostného produktu ESET nainštalovanom na počítači, na ktorom je spustené ESET SysRescue CD.

4.7.2.3 Pokročilé

Záložka **Pokročilé** vám umožňuje optimalizovať ESET SysRescue CD podľa veľkosti systémovej pamäte vo vašom počítači. Vyberte **viac alebo rovno 576 MB** pre zapísanie obsahu CD do operačnej pamäte (RAM) pri spustení. Ak vyberiete **menej ako 576 MB**, bude sa na CD neustále pristupovať počas behu WinPE.
Externé ovládače – v tejto sekcii môžete vložiť ovládače pre špecifický hardware (najčastejšie sieťová karta). Aj keď je WinPE postavený na systéme Windows Vista SP1 a má širokú podporu hardware, môže nastať situácia, že hardware nie je rozoznaný a je potrebné pridať ovládač manuálne. Pridať ovládač do kompilácie ESET SysRescue je možné dvoma spôsobmi - manuálne (tlačidlo **Pridať**) a automaticky (tlačidlo **Aut. Hľadanie**). V prípade manuálneho zadania je potrebné zvoliť cestu k .inf súboru (použiteľný *.sys súbor musí byť tiež umiestnený v rovnakom adresári). V prípade automatického nájdenia ovládača je tento automaticky nájdený v operačnom systéme daného počítača. Odporúčame použiť automatické nájdenie iba ak bude ESET SysRescue použité na počítači s rovnakým sieťovým adaptérom ako má počítač, na ktorom bolo ESET SysRescue CD vytvorené. Pri vytváraní ESET SysRescue CD je ovládač zahrnutý do kompilácie, takže používateľ ho nemusí opätovne hľadať neskôr.

4.7.2.4 Zavádzacie USB zariadenie

V prípade, že ste ako cieľové médium zvolili USB, v záložke **Zavádzacie USB zariadenie** máte možnosť zvoliť, ktoré z dostupných USB zariadení bude použité (ak ich je viac).

4.7.2.5 Napaľovanie

V prípade, že ste ako cieľové médium zvolili CD/DVD, máte možnosť nastaviť základné parametre napaľovania.
Zmazať ISO súbor – po napálení ESET SysRescue CD sa zmaže vytvorený ISO súbor
Mazanie zapnuté – je možné zvoliť rýchle zmazanie a kompletné zmazanie média
Upozornenie: Toto je prednastavená voľba. V prípade, že je použité prepisovateľné CD/DVD, budú z neho pri tomto nastavení vymazané všetky dáta.
Napaľovacia mechanika – výber mechaniky, ktorá bude použitá pri napaľovaní
V časti Médium sa nachádzajú informácie o aktuálne vloženom médiu do napaľovacej mechaniky.
Rýchlosť pálenia – môžete zvoliť požadovanú rýchlosť z roletového menu. Rozsah týchto hodnôt závisí od typu napaľovacej mechaniky a druhu použitého CD/DVD

4.7.3 Práca s ESET SysRescue

Aby bolo možné záchranné CD/DVD/USB efektívne použiť, je dôležité zabezpečiť, aby počítač nabootoval z ESET SysRescue média. Tento parameter je možné meniť v nastaveniach BIOSu (tzv. Boot priority). Druhou možnosťou je vyvolať tzv. boot menu priamo pri štarte počítača – väčšinou pomocou niektorej z kláves F9 až F12, v závislosti od výrobcu základnej dosky či verzie BIOSu.
Po nabootovaní sa spustí ESS/EAV. V tomto prostredí pochopiteľne nefungujú všetky druhy ochrán a moduly sú zredukované na položky **Kontrola počítača**, **Aktualizácia** a niektoré časti **Nastavení**. Schopnosť aktualizovať sa na najnovšiu verziu vírusovej databázy je dôležitá vlastnosť ESET SysRescue. Odporúčame program aktualizovať vždy pred spustením Kontroly počítača.

4.7.3.1 Použitie ESET SysRescue

Predpokladajme, že počítače vo firme boli napadnuté vírusom, ktorý modifikuje spustiteľné (*.exe) súbory. ESS/EAV dokáže infikované súbory vyliečiť a vírus z nich odstrániť, avšak nedokáže vyliečiť súbor *explorer.exe*, dokonca ani v Núdzovom režime.
Príčinou tohto stavu je fakt, že *explorer.exe* je jedným zo základných procesov operačného systému Windows a je spustený aj v Núdzovom režime. ESS/EAV preto na ňom nemôže vykonať žiadnu operáciu a súbor tak ostáva naďalej infikovaný.
Riešením takejto situácie je práve použitie ESET SysRescue, ktoré na svoje fungovanie nevyužíva žiadny komponent z nainštalovaného operačného systému. To mu umožňuje bez problémov manipulovať so všetkými súbormi na disku – t.j. liečiť a mazať infikované súbory.

4.8 Uživatelské prostředí

ESET Mail Security umožňuje měnit nastavení pracovního prostředí programu podle potřeby. Nastavení uživatelského prostředí programu ESET Mail Security jsou dostupné přes Pokročilé nastavení ESET Mail Security větev **Uživatelské rozhraní**.

.Část **Prvky uživatelského rozhraní** umožňuje aktivaci Rozšířeného režimu zobrazení, který obsahuje podrobnější nastavení a ovládací objekty aplikace ESET Mail Security.

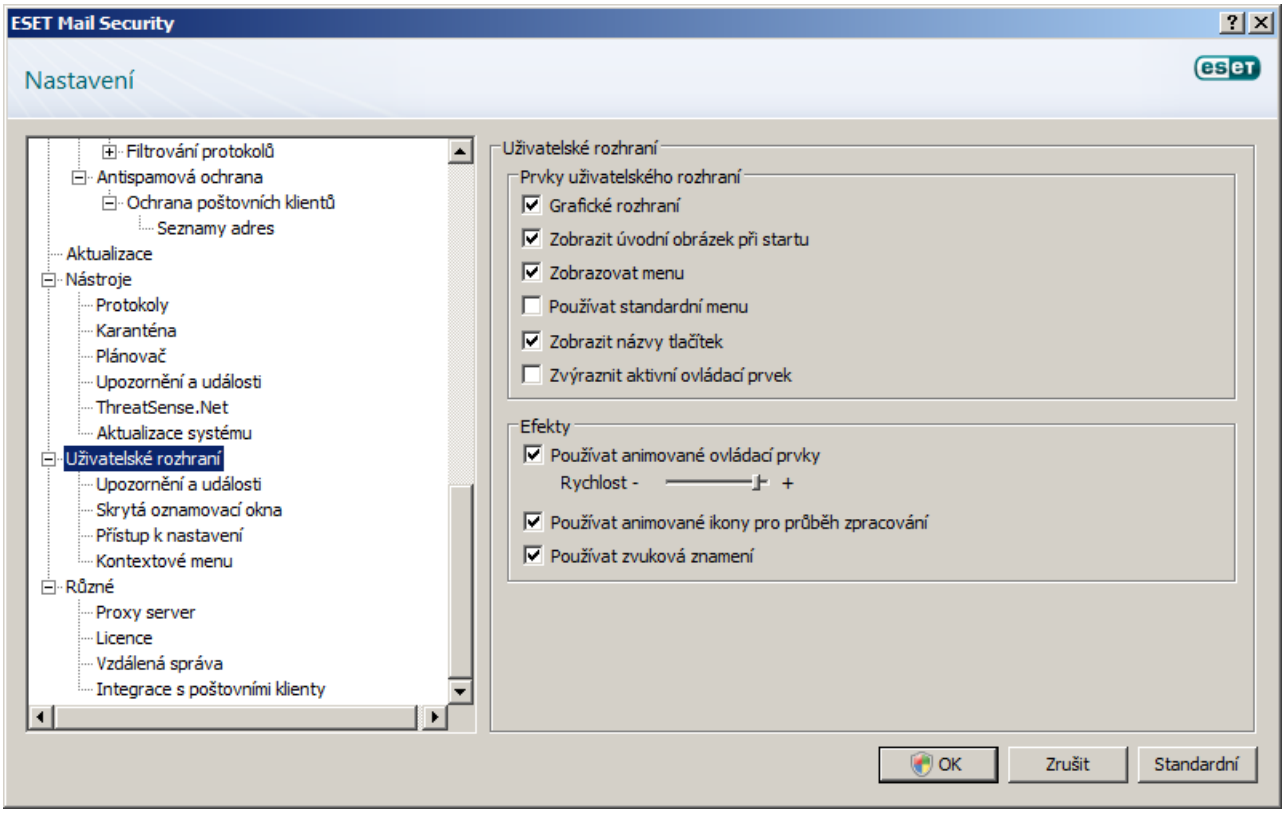
Používání grafického režimu je vhodné deaktivovat v případě, že grafika zpomaluje práci s počítačem, případně způsobuje jiné problémy. Možnost vypnutí grafického režimu je také vhodná pro zrakově postižené osoby, zejména z důvodu funkčnosti aplikací pro automatické čtení textu.

Možnost zobrazit úvodní obrázek při startu lze aktivovat výběrem možnosti se stejným názvem.

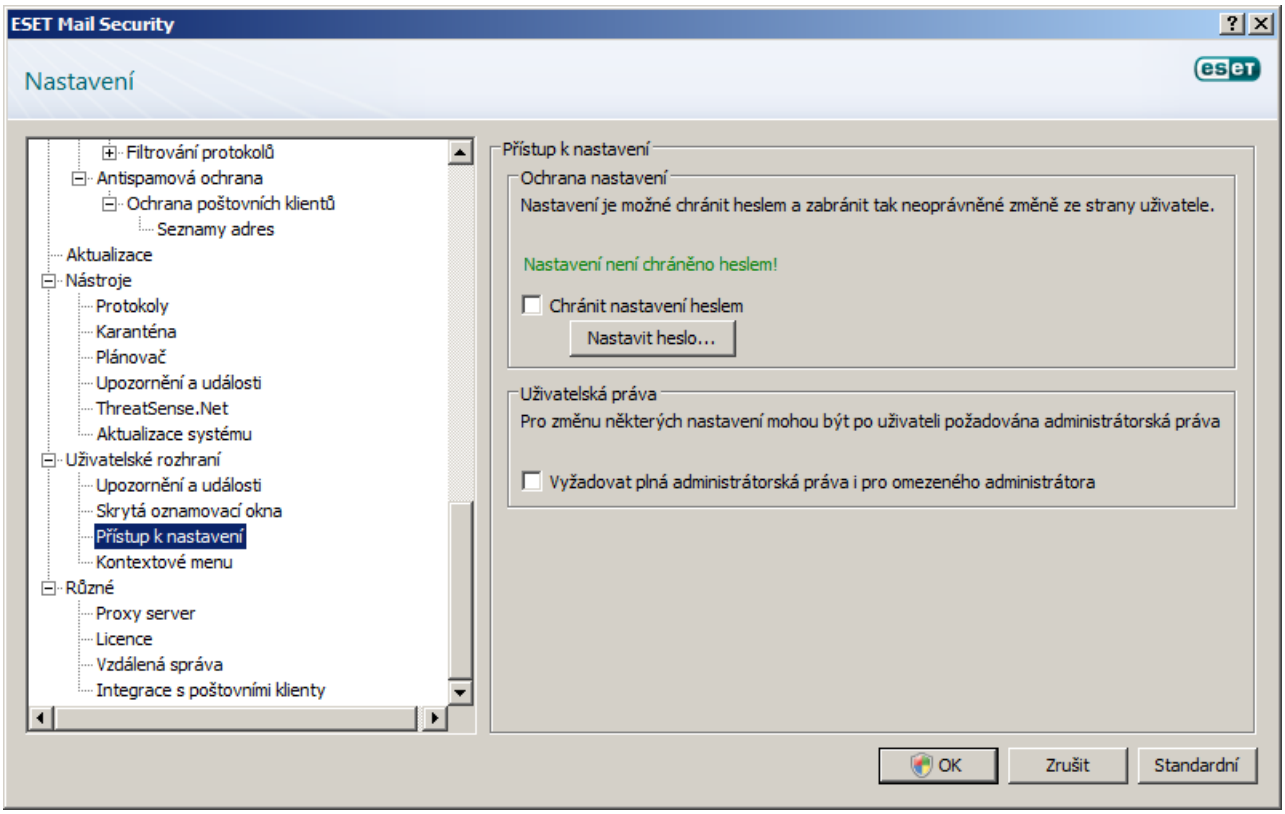
V horní části hlavního okna aplikace ESET Mail Security se nachází standardní nabídka, kterou lze zobrazit a skrýt pomocí možnosti Používat standardní menu.

Pomocí možnosti zobrazit názvy tlačítek lze aktivovat popisy, které se zobrazí, pokud uživatel na chvíli ponechá kurzor nehybně na daném tlačítku. Možnost zvýraznění aktivního ovládacího prvku aktivuje zvýrazňování prvku, který se momentálně nachází v aktivní oblasti kurzoru a bude aktivován po kliknutí.

V části **Efekty** může uživatel měnit grafické prvky rozhraní. Hlavní možností je použití grafických animovaných prvků, přičemž rychlost těchto animací je také konfigurovatelná. Lze také aktivovat používání animování ikon, které se zobrazují v průběhu zpracování úloh. Při událostech v systému mohou zaznít zvukové efekty, které mohou být zapnuty pomocí možnosti **Používat zvuková znamení.**



K nastavení rozhraní patří také možnost uzamčení nastavení aplikace ESET Mail Security. Tato možnost se nachází v podvětvi Ochrana nastavení. Správné nastavení systému je důležitým faktorem ochrany stanice a každá nechtěná změna by mohla mít vážné důsledky. Z tohoto důvodu je důležité, aby byla nastavení chráněna před zásahem neoprávněného uživatele. Rozhraní může být uzamčeno tlačítkem **Nastavit heslo** a následným zadáním hesla.



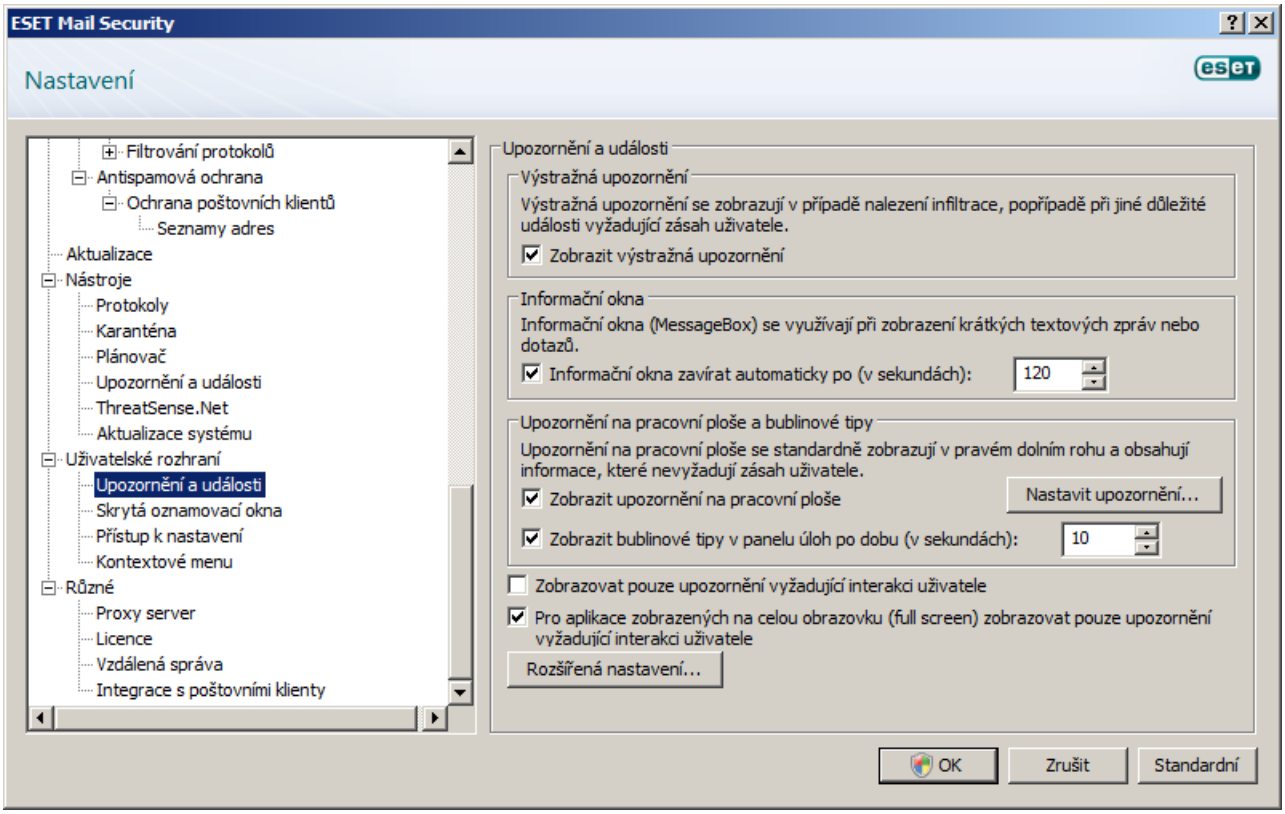
4.8.1 Upozornění a události

Pomocí dialogového okna **Upozornění a události**, které patří pod položku Uživatelské rozhraní (viz výše), lze nakonfigurovat výstražná a informační hlášení aplikace ESET Mail Security.

Jako první je uvedena položka **Zobrazit výstražná upozornění**. Její vypnutí způsobí, že se nebudou zobrazovat výstražná okna, což je vhodné aplikovat pouze na úzký okruh specifických situací. Většině uživatelů se doporučuje ponechat tuto možnost aktivní.

Délku zobrazení informačních oken ovlivňuje prvek Informační okna zavírat automaticky po (v sekundách). Po uplynutí nastaveného časového intervalu se okno s upozorněním zavře, pokud to již neprovedl sám uživatel.

Upozornění na pracovní ploše a bublinové tipy jsou informačními prostředky, které nenabízejí ani nevyžadují zásah uživatele. Zobrazují se v pravém dolním rohu obrazovky. Zobrazování upozornění na pracovní ploše je aktivováno pomocí možnosti **Zobrazit upozornění na pracovní ploše**, přičemž podrobnější možnosti, jako je délka zobrazení upozornění nebo průhlednost tohoto okna, může uživatel změnit pomocí tlačítka **Nastavit upozornění**. V tomto dialogovém okně si můžete prohlédnout ukázku nastavení klepnutím na tlačítko Ukázka. U bublinových tipů lze konfigurovat délku zobrazení pomocí možnosti **Zobrazit bublinové tipy v panelu úloh po dobu (v sekundách)**.



V dolní části okna **Upozornění a události** se nachází možnost **Zobrazit pouze upozornění vyžadující zásah uživatele**. Po aktivaci této možnosti se budou zobrazovat pouze hlášení, která vyžadují aktivní účast uživatele a čekají na jeho pokyn. Poslední možností konfigurace v tomto okně je nastavení příjemce zpráv ve víceuživatelských systémech. Tato položka má název Ve víceuživatelském prostředí zasílat systémová hlášení uživateli a specifikuje jméno uživatele, kterému budou zasílána důležitá systémová hlášení. Standardně je tímto uživatelem správce systému nebo sítě. Tuto možnost je vhodné použít na terminálovém serveru, kde všechna systémová hlášení budou zasílána pouze správci.

4.8.2 Deaktivace grafického rozhraní

Tato kapitola popisuje, jak deaktivovat grafické rozhraní (GUI) programu ESET Mail Security pro uživatele přihlášené na terminálovém serveru.

Za normálních okolností se grafické rozhraní (GUI) ESET Mail Security spustí při každém přihlášení uživatele na Terminálový server. Toto je většinou nežádoucí, pokud se jedná o Terminálový server a běžné uživatele, kteří nemají mít přístup k programu ESET Mail Security a jeho nastavením. Pokud chcete vypnout GUI pro Terminálové připojení, proveďte následující kroky:

1. Spustit *regedit.exe*
2. Větev *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*
3. Kliknout pravým tlačítkem na položku *egui* a zvolit *Modify…*
4. Přidat přepínač `/terminal` na konec existujícího řetězce.

Příklad pole *Value data* položky *egui*:

```
"C:\Program Files\ESET\ESET Mail Security\egui.exe" /hide /waitservice /terminal
```

Pokud si přejete vrátit původní nastavení a tím opět zprovoznit automatické spouštění grafické rozhraní (GUI) ESET Mail Security, odeberte přepínač `/terminal`. Pro přístup k položce egui v registrech opakujte kroky 1. až 3.

4.9 Kontrola z příkazového řádku

Antivirový modul ESET Mail Security lze spustit také přes příkazový řádek – manuálně (příkazem „ecls“) nebo pomocí souboru typu „bat“.

Při spouštění skeneru na vyžádání přes příkazový řádek můžete použít několik parametrů a přepínačů:

Všeobecné:

– help	zobrazení nápovědy
– version	zobrazení verze skeneru
– base-dir = FOLDER	nahrání modulů ze složky FOLDER
– quar-dir = FOLDER	uložení složky FOLDER do karantény
– aind	zobrazení ukazatele průběhu kontroly

Cíle:

– files	kontrola souborů (standardně)
– no-files	nekontrolování souborů
– boots	kontrola boot sektorů (standardně)
– no boots	nekontrolování boot sektorů
– arch	kontrola archívů (standardně)
– no-arch	nekontrolování archívů
– max-archive-level = LEVEL	úroveň hloubky kontroly vnořených archívů
– scan-timeout = LIMIT	LIMIT je maximální čas (v sekundách) kontroly archívů. Pokud čas kontroly přesáhne tento limit, kontrola archivu se přeruší a pokračuje následujícím souborem.
– max-arch-size = SIZE	SIZE je počet prvních bajtů archivu, které se mají zkontrolovat(standardně 0 = bez omezení)
– mail	kontrola emailových souborů
– no-mail	nekontrolování emailových souborů
– sfx	kontrola samorozbalovacích archívů
– no-sfx	nekontrolování samorozbalovacích archívů
– rtp	kontrola runtime archívů
– no-rtp	nekontrolování runtime archívů
– exclude = FOLDER	vyloučení složky FOLDER z kontroly
– subdir	zapnutí kontroly podsložek (standardně)
– no-subdir	vypnutí kontroly podsložek
– max-subdir-level=LEVEL	úroveň kontroly podsložek (standardně 0 – bez omezení)
– symlink	následování symbolického odkazu (standardně)
– no-symlink	ignorování symbolického odkazu
– ext-remove = EXTENSIONS	
– ext-exclude = EXTENSIONS	vyloučení souborů s koncovkou uvedenou v seznamu (koncovky oddělit dvojtečkou)

Metody:

– adware	zapnutí detekce Adware/Spyware Riskware
– no-adware	vypnutí detekce Adware/Spyware Riskware
– unsafe	zapnutí detekce potenciálně nebezpečných aplikací
– no-unsafe	vypnutí detekce potenciálně nebezpečných aplikací
– unwanted	zapnutí detekce potenciálně nechtěných aplikací
– no-unwanted	vypnutí detekce potenciálně nechtěných aplikací
– pattern	zapnutí použití vzorek při detekci
– no-pattern	vypnutí použití vzorek při detekci
– heur	zapnutí použití heuristiky při detekci
– no-heur	vypnutí použití heuristiky při detekci
– adv-heur	zapnutí použití rozšířené heuristiky při detekci
– no-adv-heur	vypnutí použití rozšířené heuristiky při detekci

Léčení:

– action = ACTION	akce, která má být provedena na infikovaných souborech. Možnosti: none, clean, prompt
– quarantine	kopírování infikovaných souborů do karantény (doplněk k přepínači action)
– no-quarantine	nekopírovat infikované soubory do karantény

Protokoly:

– log-file = FILE	uložení výsledků kontroly do protokolu souboru FILE
– log-rewrite	přepsání původního souboru (standardně: připojení k původnímu log souboru)
– log-all	zaznamená vše
– no-log-all	zaznamená pouze infikované soubory (standardně)

Kontrola může končit následujícími výstupními kódy:

0	– nebyla nalezena žádná infiltrace
1	– byla nalezena infiltrace, nebyla však odstraněna
10	– v počítači ještě zůstali infikované soubory
101	– chyba při kontrole archivu
102	– chyba při přístupu k souboru

103 – interní chyba

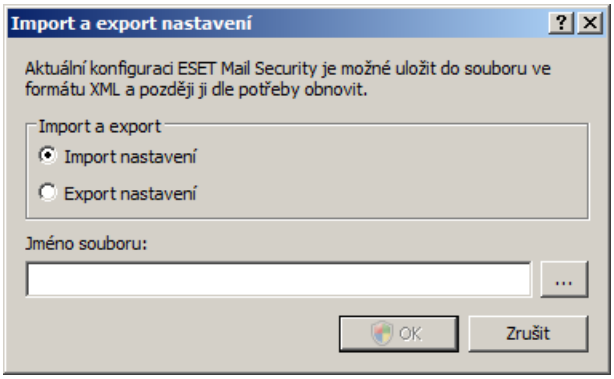
POZNÁMKA: Výstupní kódy vyšší než 100 znamenají, že soubor nebyl zkontrolován a může být infikován.

4.10 Import a Export nastavení

Import a export nastavení ESET Mail Security je přístupný v části **Nastavení**.

Při exportu se uloží všechna nastavení ESET Mail Security.

Import a export nastavení využívá soubory typu XML. Export a import nastavení je užitečný např. pokud potřebujete zálohovat nastavení ESET Mail Security a později nastavení využít.



4.11 ThreatSense.Net

Systém včasného varování ESET Mail Security je nástroj, který zabezpečuje pohotovou a neustálou informovanost společnosti ESET o nových infiltracích. Obousměrný Systém včasného varování má jediný účel – zvýšit ochranu, kterou vám poskytujeme. Nejlepší způsob, kterým můžeme zajistit, abychom měli k dispozici všechny nové infiltrace v době jejich vzniku, je obrátit se na co největší počet našich zákazníků a využít je jako „průzkumníky". Máte dvě možnosti:

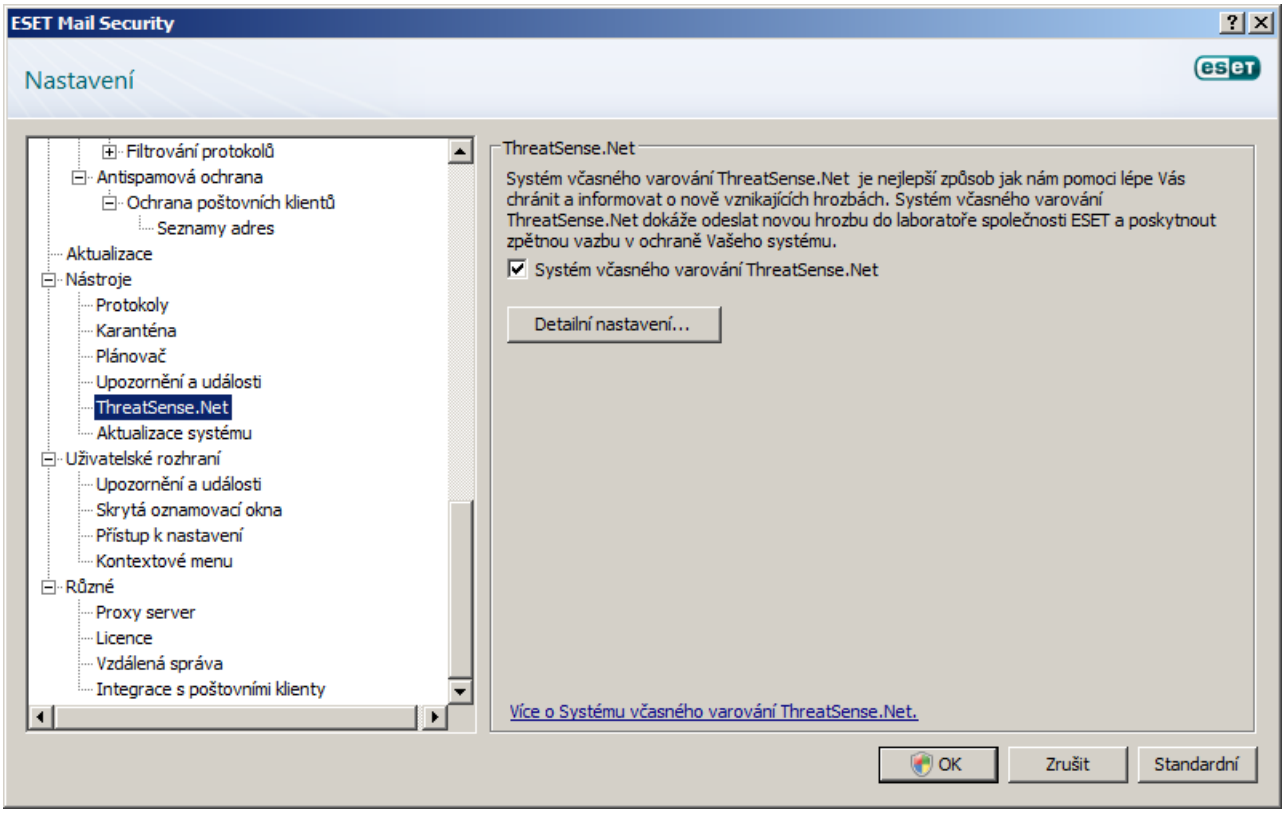
1. Můžete se rozhodnout Systém včasného varování neaktivovat. Budete mít stále k dispozici všechny funkce aplikace i nejvyšší ochranu, kterou dokážeme poskytnout.

2. Můžete se rozhodnout Systém včasného varování aktivovat. V takovém případě je možné odesílat informace o nových infiltracích. Pokud je nový nebezpečný kód součástí souboru, bude celý soubor odeslán k podrobné analýze do společnosti ESET, spol. s r.o. Prostudování těchto infiltrací nám pomůže zvýšit schopnosti detekce. Systém včasného varování shromáždí z vašeho počítače ty informace, které se týkají nové infiltrace. Mezi ně může patřit ukázka nebo kopie souboru, v němž se infiltrace objevila; název adresáře, kde se soubor nacházel; název souboru; informace o datu a čase detekce; způsob, kterým se infiltrace dostala do vašeho počítače; a informace o operačním systému vašeho počítače. Některé z těchto informací mohou obsahovat osobní údaje o uživateli počítače, například pokud je jeho jméno součástí názvu adresáře apod.

Existuje tedy možnost, že za jistých okolností se nějaká informace o vás nebo vašem počítači dostane do laboratoří společnosti ESET, spol. s r.o. Nemáme však v úmyslu získávat takové informace za žádným jiným účelem než zabezpečit okamžitou reakci na nové infiltrace.

Podle standardních výchozích nastavení se aplikace ESET Mail Security zeptá, zda chcete podezřelý soubor odeslat k podrobné analýze do laboratoří společnosti ESET, spol. s r.o. Pokud je infiltrace nalezena v souborech s určitými příponami, jako například .doc a .xls, nikdy se neodesílá jejich obsah. Pokud existují další soubory, které nechcete odesílat, můžete doplnit další přípony.

Nastavení ThreatSense.Net jsou k dispozici ze stromu pokročilých nastavení pomocí příkazu **Nástroje-ThreatSense.Net**. Po zaškrtnutí políčka Systém včasného varování ThreatSense.Net můžete vstoupit do nastavení systému.

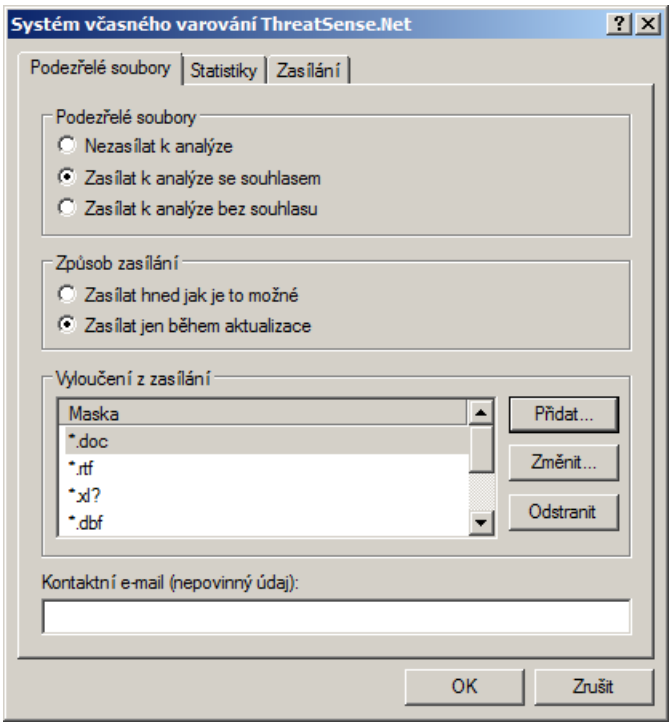


4.11.1 Podezřelé soubory

Jako **podezřelé soubory** jsou označovány dosud neznámé infiltrace, které byly detekovány rozšířenou heuristikou antivirového skeneru.

V případě, že máte soubor s podezřelým chováním, můžete nám jej zaslat k analýze do naší virové laboratoře. Pokud se ukáže, že jde o nebezpečnou aplikaci, bude její detekce přidána do některé nejbližší aktualizace.

Zasílání souborů lze nastavit tak, aby fungovalo plně automaticky bez zásahu uživatele. V tomto případě budou podezřelé soubory zasílány na pozadí. Chcete-li vědět, které soubory budou zaslány, nebo si přejete odeslání nejprve potvrdit, vyberte možnost **Zasílat k analýze s potvrzováním souborů**.



Chcete-li, aby k analýze nebyly zasílány žádné soubory, můžete nastavit i tuto možnost. Je třeba podotknout, že možnost nezasílat soubory k analýze nemá vliv na zasílání statistických informací do společnosti ESET, spol. s r.o. Statistické informace 106 se nastavují pomocí vlastních nastavení, která jsou uvedena v následující kapitole.

Způsob zasílání - Podezřelé soubory mohou být zaslány ihned, jakmile jsou detekovány. Toto nastavení je doporučeno, pokud máte pevné připojení k Internetu a chcete, aby podezřelé soubory byly doručeny neprodleně. Další možností je zasílání podezřelých souborů v průběhu aktualizace programu. V takovém případě v rámci připojení na aktualizační servery proběhne také přenos podezřelých souborů na servery Systému včasného varování.

Výjimky - K analýze nemusejí být zasílány všechny druhy souborů. Přejete-li si, aby nebyly zasílány soubory s citlivými daty, můžete jejich zasílání vyloučit. Do této skupiny můžete zařadit ty typy souborů, ve kterých se obvykle nacházejí důvěrné informace, například textové dokumenty a tabulky. Standardně jsou vyloučeny typy souborů aplikace Microsoft Office a OpenOffice. Seznam lze průběžně upravovat.

Kontaktní e-mail - Umožňuje zadat nepovinný kontaktní e-mail, na který se mohou analytici společnosti ESET, spol. s r.o. ve výjimečných situacích obrátit, kdyby potřebovali doplňující informace ohledně infikovaného souboru. Většina odeslaných souborů bude ovšem zpracována automaticky, bez osobní zpětné vazby.

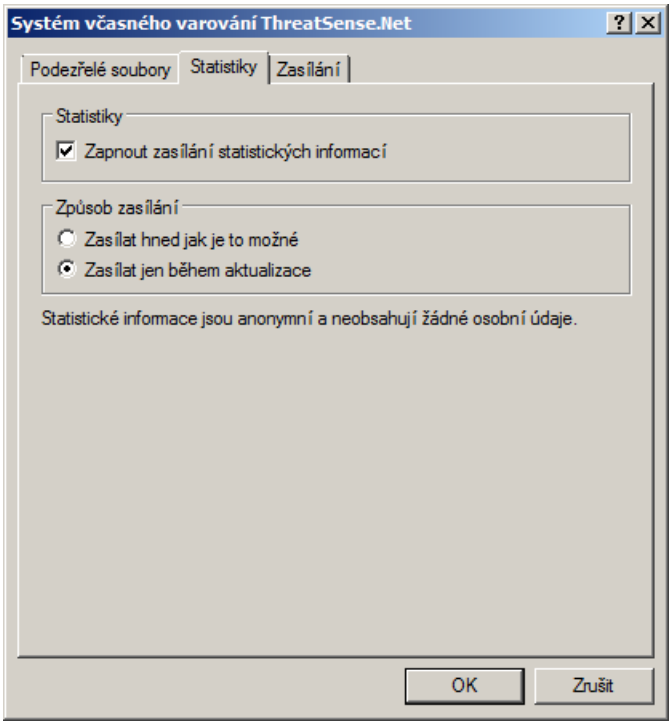
4.11.2 Statistiky

Systém včasného varování ThreatSense.Net shromažďuje anonymní informace o vašem počítači, které souvisejí s nově zjištěnými hrozbami. Ty mohou obsahovat název infiltrace, datum a čas detekce, verzi systému ESET Mail Security, verzi používaného operačního systému a místní nastavení. Statistiky se běžně odesílají na servery společnosti ESET, spol. s r.o. jednou až dvakrát denně.

Příklad statistických informací odesílaných do společnosti ESET, spol. s r.o.:

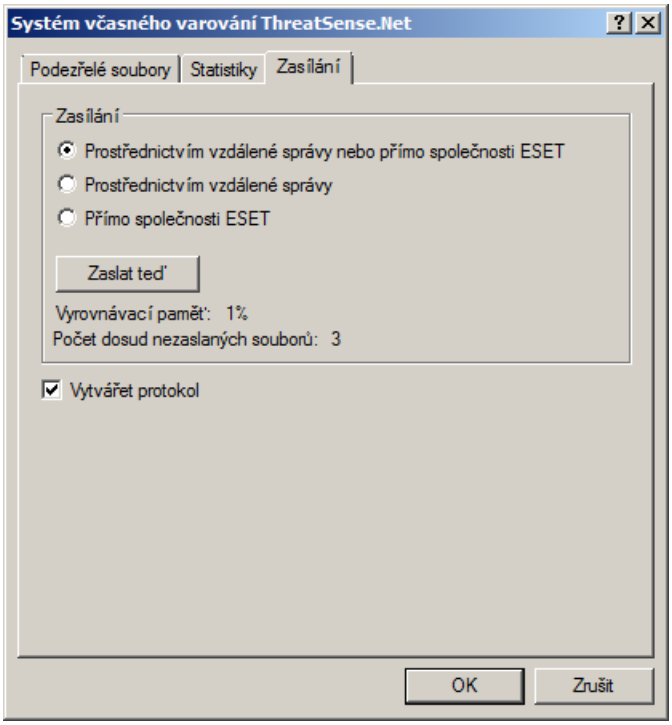
```
# utc_time=2005-04-14 07:21:28
# country="Slovakia"
# language="ENGLISH"
# osver=5.1.2600 NT
# engine=5417
# components=2.50.2
# moduleid=0x4e4f4d41
# filesize=28368
# filename=C:\Documents and Settings\Administrator\
Local Settings\Temporary Internet Files\Content.IE5\
C14J8NS7\rdgFR1463[1].exe
```

Způsob zasílání - V části Způsob zasílání můžete nastavit, kdy bude program zasílat statistické informace. Pokud zvolíte možnost zasílání ihned, jakmile je to možné, statistické informace budou zasílány co nejdříve po vytvoření. Toto nastavení je vhodné, pokud máte pevné připojení k Internetu. Vyberete-li možnost zasílání pouze v průběhu aktualizace, budou statistické informace uchovávány a budou odeslány najednou v průběhu aktualizace.



4.11.3 Posílání

V této části můžete nastavit, zda soubory a statistické informace budou zasílány **Prostřednictvím vzdálené správy** počítačů, nebo **Přímo společnosti ESET**. Pokud chcete mít jistotu, že podezřelé soubory a statistické informace budou do společnosti ESET, spol. s r.o. doručeny, vyberte možnost zasílání **Prostřednictvím vzdálené správy nebo Přímo společnosti ESET**. V takovém případě budou soubory a statistiky zasílány všemi dostupnými prostředky. Zasílání podezřelých souborů prostřednictvím vzdálené správy odešle soubory a statistiky na server vzdálené správy, která zabezpečí jejich následné odeslání do virové laboratoře společnosti ESET, spol. s r.o. Možnost zasílání souborů přímo společnosti ESET doručí podezřelé soubory a statistiky přímo do virové laboratoře.



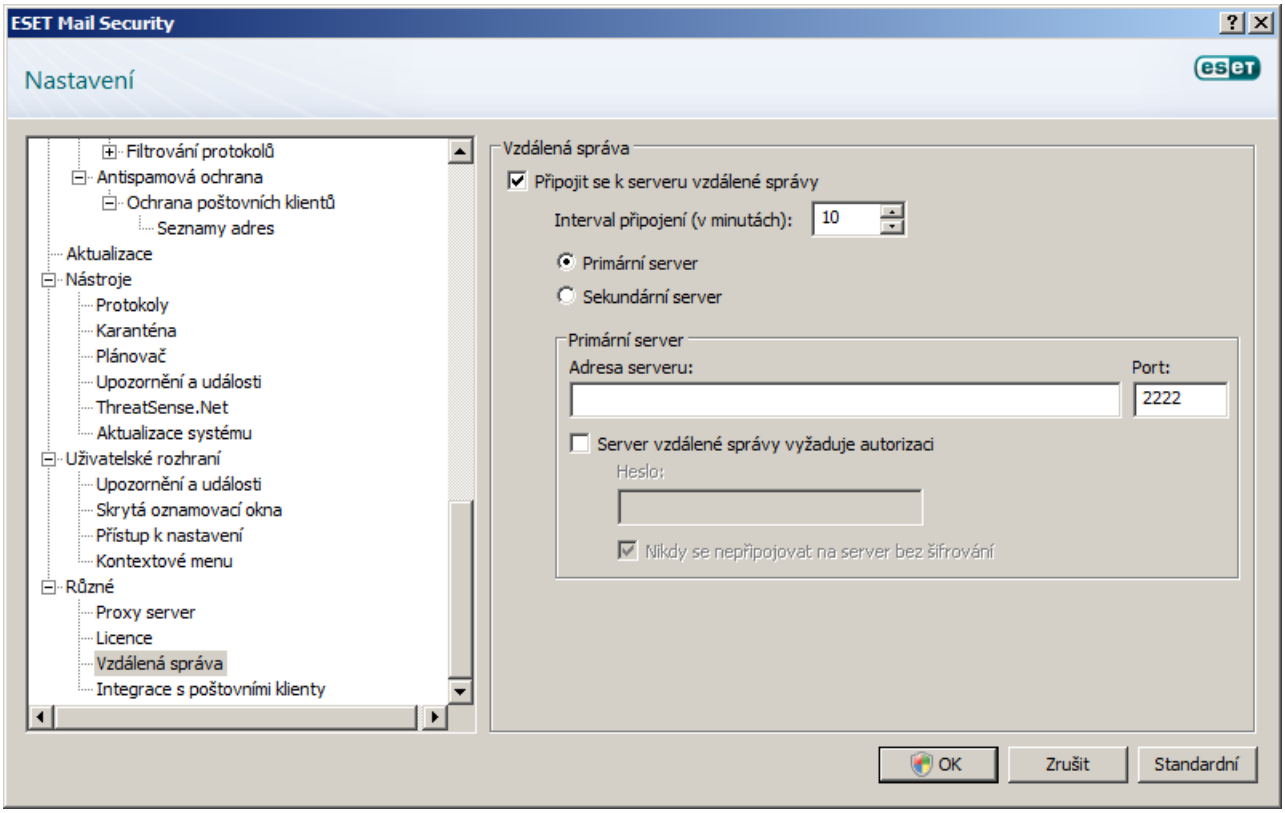
V případě, že se v počítači nacházejí soubory čekající na zaslání, bude v nastaveních zasílání k dispozici tlačítko **Zaslat nyní**. Můžete jej použít, pokud chcete, aby soubory nebo statistické informace byly zaslány ihned.

Zaškrtnutím políčka **Vytvořit protokol** povolíte, aby události zasílání souborů a informací byly zaznamenávány. Po každém odeslání podezřelého souboru a statistických informací se vytvoří záznam v protokolu událostí.

4.12 Vzdálená správa

ESET Remote Administrator je velmi účinný nástroj na údržbu uplatňování bezpečnostních zásad a přehlednosti v celkové správě bezpečnosti celé sítě. Její použití je vhodné v každé větší síti, protože kromě zvýšení bezpečnosti znamená také usnadnění správy aplikace ESET Smart Security nebo ESET NOD32 Antivirus na klientských počítačích.

Dialog s nastavením vzdálené správy je dostupný z hlavního okna aplikace ESET Mail Security pomocí odkazů **Nastavení** > **Zobrazit celý strom pokročilého nastavení** > **Různé** > **Vzdálená správa**.



Samotné okno především nabízí aktivaci režimu vzdálené správy, kterou lze provést zaškrtnutím políčka **Připojovat se k serveru vzdálené správy**. Poté budou přístupné i ostatní možnosti okna, jejichž popis následuje:

- **Interval připojování (v minutách):** čas, který uplyne mezi dvěma po sobě následujícími připojeními klienta na server. Jinými slovy, klient bude odesílat informace na server v časových intervalech určených touto hodnotou. V případě nastavení hodnoty O budou informace odesílány každých 5 sekund.

- **Adresa serveru:** síťová adresa serveru, na kterém je nainstalovaný server vzdálené správy.

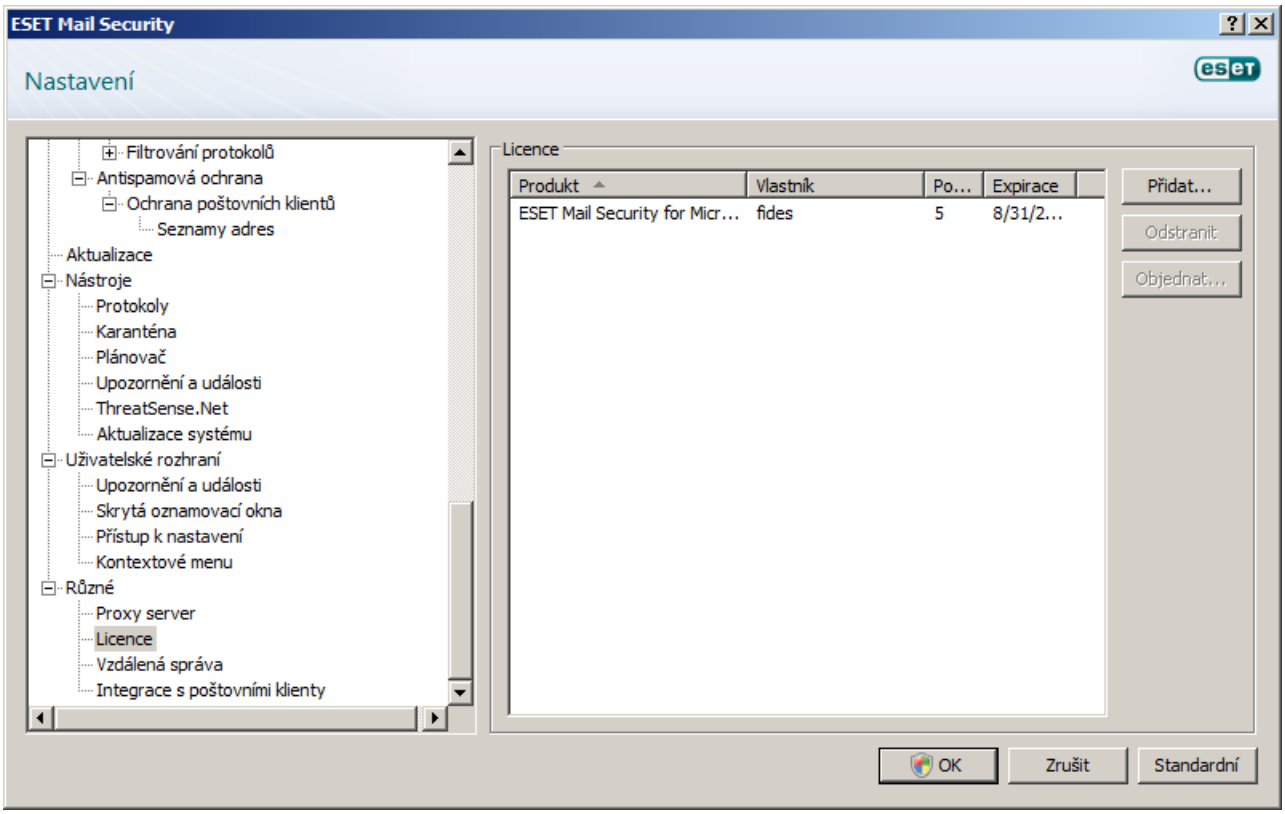
- **Port:** číslo portu serveru, na který se bude klient připojovat. Doporučujeme použít přednastavenou standardní hodnotu 2222.

- **Server vzdálené správy vyžaduje autorizaci:** v případě přihlašování na server vzdálené správy, který je zabezpečený heslem, je potřeba zadat požadované heslo do pole **Heslo:**.

Po klepnutí na tlačítko **OK** se změny uloží a aplikace ESET Mail Security se bude na vzdálený server připojovat podle nastavení.

4.13 Licence

Položka **Licence** vám umožňuje správu licenčních klíčů for ESET Mail Security a také pro některé ostatní produkty firmy ESET, spol s.r.o jako např. ESET Mail Security. Klíč je dodáván spolu s autorizačními po zakoupení produktu. Přidání licencí do programu se provádí přes licenční manažer, který je přístupný pokročilých nastavení, v části **Různé** > **Licence.**



Licenční klíč je textový soubor obsahující informace o produktu, pro který byl klíč vydán, a také o jeho vlastníkovi, počtu licencí a vypršení platnosti licenčního klíče.

Okno správce licencí umožňuje načíst obsah licenčního klíče pomocí tlačítka **Přidat...** a zobrazit tak informace, které licenční klíč obsahuje. Licenční klíč lze odstranit pomocí tlačítka **Odstranit**.

Pokud vypršela platnost licenčního klíče, tj. je ukončena doba jeho platnosti, je v případě zájmu možné zakoupit příslušný produkt pomocí tlačítka **Objednat...** – budete přesměrováni na stránku elektronického obchodu.

5. Slovník

5.1 Typy infiltrací

Jako infiltrace je označován škodlivý software, který se snaží proniknout do počítače a vykonávat škodlivou činnost.

5.1.1 Viry

Tento druh infiltrací obvykle napadá již existující soubory na disku. Pojmenován byl podle biologického viru, protože se z počítače na počítač šíří obdobným způsobem.

Počítačové viry napadají nejčastěji spustitelné soubory a dokumenty. Děje se to tak, že „tělo" viru se k nim připojí – obvykle na konec souboru. Průběh aktivace počítačového viru je tedy zhruba následující: po spuštění napadeného souboru nejprve dojde ke spuštění připojeného viru. Ten vykoná akci, kterou má v sobě naprogramovanou. A až nakonec se ke slovu dostane původní aplikace.

Vlastní činnost aktivovaného viru může mít mnoho podob. Některé viry jsou krajně nebezpečné, protože dokáží cíleně smazat soubory z disku, na druhé straně jiné mají pouze zdůraznit zručnost svých tvůrců a uživatele spíše obtěžují, než aby způsobovaly reálnou škodu.

Je třeba říci, že viry jsou (na rozdíl od trojských koní či spywaru) v dnešní době čím dál tím vzácnější, protože jsou pro své tvůrce komerčně nezajímavé. Pojem virus se často nesprávně používá pro označení všech druhů infiltrací. V současnosti se již od tohoto pojmenování upouští a prosazuje se výstižnější a správnější společný název „škodlivý software" (malware).

V případě infikování virem je třeba napadený soubor vrátit do původní podoby, tedy vyléčit jej pomocí antivirového systému.

Příklady virů: *OneHalf*, *Tenga*, *Yankee Doodle*.

5.1.2 Červi

Počítačový červ je program obsahující škodlivý kód, který napadá hostitelské počítače a šíří se dál prostřednictvím sítě. Základní rozdíl mezi virem a červem je ten, že červ se dokáže šířit sám a není závislý na hostitelském souboru (či boot sektoru disku). Červ využívá k šíření hlavně elektronickou poštu nebo síťové pakety.
Červi se proto dělí na základě způsobu šíření na:

- **e-mailové** – rozesílají se na e-mailové adresy, které najdou v adresáři hostitelského systému.
- **síťové** – zneužívají bezpečnostní díry v různých aplikacích.

Červ je tedy mnohem životaschopnější než virus. Díky značnému rozšíření Internetu se červ dokáže dostat do celého světa během několika hodin od vydání, v některých případech dokonce v průběhu několika minut – a proto je nebezpečnější. Aktivovaný červ v systému dokáže způsobit celou řadu nepříjemností – od mazání souborů, přes značné zpomalení činnosti počítače, až po deaktivaci některých programů. Díky svému charakteru je ideální jako "pomoc" při distribuci jiných druhů infi ltrací. V případě infekce červem se doporučuje škodlivý soubor odstranit, protože obsahuje pouze škodlivý kód.

Příklady známých červů: *Lovsan/Blaster*, *Stration/Warezov*, *Bagle*, *Netsky*.

5.1.3 Trojské koně

Počítačové trojské koně jsou typem infiltrace, které se snažili maskovat za užitečné programy, aby tak zajistili své spuštění uživatelem. Je potřeba poznamenat, že to platilo pro počítačové trojské koně v minulosti. Dnes se již takto obvykle neprezentují a jejich hlavním cílem je získat snadný přístup do systému, aby tam mohli vykonávat škodlivou činnost. Termín trojský kůň je v současnosti obecný pojem, kterým je označovaná v podstatě jakákoli infiltrace, kterou nelze zařadit do jiné kategorie. Vzhledem k tomu, že se jedná o poměrně širokou kategorii aplikací, existuje řada poddruhů. Mezi nejznámější patří:

- **Downloader** – Škodlivý kód, jehož úlohou je z Internetu stahovat do systému další infi ltrace
- **Dropper** – tzv. nosič. Přenáší v sobě ukrytý další škodlivý software (např. viry) a ztěžují tím jejich detekci antivirovými programy
- **Backdoor** – tzv. zadní dvířka. Je to program komunikující se vzdáleným útočníkem, který tak může získat přístup a kontrolu nad napadnutým systémem
- **Keylogger** – sleduje, jaké klávesy uživatel stisknul a odesílá informace vzdálenému útočníkovi
- **Dialer** – připojuje se na zahraniční telefonní čísla, které jsou zpoplatněny vysokými částkami. Uživatel prakticky nemá šanci zaregistrovat odpojení od místního poskytovatele připojení a vytvoření nového připojení do zahraničí. Reálnou škodu mohou tyto programy způsobit pouze uživatelům s vytáčeným připojením (tzv. dial-up)

Trojské koně se nejčastěji vyskytují ve formě spustitelného souboru s příponou „.exe“. Soubor neobsahuje v podstatě nic jiného než samotný škodlivý kód, proto je v případě infekce doporučenou akcí jeho smazání.

Příklady trojských koní: *NetBus*, *Trojandownloader.Small.ZL*, *Slapper*

5.1.4 Rootkits

Rootkit je kategóriou škodlivého software, ktorý zabezpečí útočníkovi prienik do systému, pričom utají svoju prítomnosť. Ide o program, ktorý po preniknutí do systému (zvyčajne využijúc nejakú bezpečnostú dieru) po sebe zahladí všetky stopy – prítomnosť súborov, spustené procesy, zápisy v registroch Windows, atď. Tým pádom je v podstate neodhaliteľný bežnou kontrolou.

Pri prevencii je potrebné vziať na vedomie fakt, že s rootkitom je možné prísť do kontaktu na dvoch úrovniach:

1) V momente, keď sa snaží preniknúť z Internetu. V tomto prípade sa ešte nenachádza v systéme, čiže je to ešte len potenciálny rootkit a antivírový systém si s ním poradí (za predpokladu, že rozpozná, že ide o infiltráciu).

2) Keď je už zavedený v systéme. Vtedy je v podstate štandardným spôsobom nedetekovateľný. Používatelia ESET Mail Security však majú výhodu v tom, že tento program používa technológiu Antistealth a dokáže aj aktívne rootkity odhaliť a eliminovať

5.1.5 Adware

Adware je zkratka termínu „advertising-supported software“. Do této kategorie patří programy, jejichž úkolem je zobrazovat reklamy. Adware obvykle sám otevře nové okno (tzv. automaticky otevírané okno) s reklamou v internetovém prohlížeči nebo změní nastavení výchozí domovské stránky. Používají jej často výrobci volně šiřitelných(bezplatných) programů, aby si finančně zajistili vývoj vlastní, v mnoha případech užitečné aplikace. Adware sám o sobě nebývá škodlivý, pouze uživatele obtěžuje.Nebezpečí spočívá v tom, že bývá často spojen se spywarem.

Pokud se uživatel rozhodne pro volně šiřitelný software, doporučuje se věnovat procesu instalace zvýšenou pozornost.Instalační program totiž často upozorňuje na to, že se spolu se zvoleným programem nainstaluje také adware, a uživatel má často možnost jeho instalaci zakázat. Některé programy ovšem bez přídavného adwaru nebude možné nainstalovat nebo budou mít omezenou funkčnost. Z toho vyplývá, že adware se může do systému dostat „legální“ cestou, protože s tím uživatel souhlasí. Pozornost je tedy namístě.

Infikovaný soubor neobsahuje v podstatě nic jiného než samotný škodlivý kód, proto je v případě infekce doporučenou akcí smazání.

5.1.6 Spyware

Kategorie spywaru zahrnuje programy, které odesílají informace bez vědomí uživatele. Odesílány jsou různé statistické informace, jako například seznam navštěvovaných internetových stránek, seznam e-mailových adres v adresáři nebo klávesy stisknuté uživatelem.

Tvůrci těchto programů argumentují tím, že se pouze snaží zjistit potřeby nebo zájmy uživatele a zásobovat ho cílenou reklamou. Hranice zneužitelnosti je však v tomto případě velmi nejasná a nelze zaručit, že získané informace nebudou v budoucnosti zneužity. Údaje získané metodami spywaru totiž mohou obsahovat různé bezpečnostní kódy, čísla bankovních účtů atd. Spyware se šíří společně s některými volně šiřitelnými programy, jejichž autoři o této skutečnosti vědí a často o tom informují uživatele během instalace.
Tím pádem jde do velké míry i o etický problém.

Příkladem volně šiřitelného softwaru obsahujícího spyware jsou hlavně klientské aplikace sítí P2P (peer-to-peer) – *Kazaa*, *BearShare*. Zvláštní podkategorií jsou programy, které se vydávají za antispyware, přičemž samy obsahují spyware – např. *Spyfalcon*, *Spy Sheriff*.

Infikovaný soubor neobsahuje v podstatě nic jiného než samotný škodlivý kód, proto je v případě infekce doporučenou akcí smazání.

5.1.7 Zneužitelné aplikace

Existuje řada programů, které za běžných podmínek slouží uživatelům k ulehčení činnosti, správě počítačových sítí apod. V nesprávných rukách však mohou být zneužity k nekalým účelům. Proto společnost ESET vytvořila tuto speciální kategorii. Uživatelé mají možnost zvolit, zda chtějí, aby antivirový program společnosti ESET tyto potenciální hrozby detekoval nebo je ignoroval.

V převážné většině se jedná o komerční a legitimní software. Může se například jednat o aplikace pro zobrazení vzdálené pracovní plochy (WinVNC), programy pro dešifrování kódů a hesel nebo tzv. keyloggery (programy na monitorování stisknutých kláves).

V případě, že uživatel zjistí přítomnost zneužitelné aplikace, která se v systému nachází bez jeho vědomí, doporučuje se (po případné poradě se správcem sítě) příslušnou aplikaci odstranit.

5.1.8 Nechtěné aplikace

Nechtěné aplikace jsou programy, které sice nemusí představovat bezpečnostní riziko, avšak mohou mít určitý vliv na činnost počítačového systému. Tyto aplikace se obvykle do systému mohou nainstalovat až po souhlasu uživatele. Jejich instalací dojde k určitým změnám v chování počítačového systému oproti stavu bez instalace příslušné aplikace. Mezi tyto změny v systému patří zejména:

- zobrazování oken, které by se jinak nezobrazovali
- aktivace a spuštění procesů, které jsou uživateli skryty
- zvýšená spotřeba systémových prostředků
- změny výsledků vyhledávání
- komunikace se servery poskytovatele aplikace

5.2 Elektronická pošta

Elektronická pošta, tedy email přináší jako moderní forma komunikace spoustu výhod. Je flexibilní, rychlá a adresná. Byla vlastně hlavním důvodem, proč se Internet v první polovině devadesátých let rozšířil po celém světě. Díky vysoké míře anonymity vznikl prostor pro zneužívání Internetu a elektronické pošty k nekalým účelům - šíření nevyžádané pošty.

Nevyžádaná pošta je poměrně širokou kategorií zahrnující například reklamy, fámy, šíření škodlivého software (malware). Nebezpečí umocňuje fakt, že náklady na rozesílání jsou v podstatě nulové a tvůrci mají k dispozici spoustu nástrojů a zdrojů na zjištění e-mailových adres. Množství nevyžádané pošty se tím stává těžko regulovatelné a běžný uživatel elektronické pošty je v podstatě neustále vystavován nebezpečným útokům. Čím déle je e-mailová schránka používána, tím se zvyšuje pravděpodobnost, že se dostane do databáze tvůrců pošty. Několik tipů na prevenci:

- pokud je to možné, nezveřejňujte svou adresu na Internetu
- poskytovat svou adresu co nejméně
- používat ne úplně běžné aliasy - složitější jsou obtížněji zjistitelné technikami používanými při rozesílání nevyžádané pošty
- neodpovídat na nevyžádanou poštu, která se do schránky již dostala
- věnovat pozornost vyplňování formulářů na Internetu - položky typu "chci dostávat do své schránky informace"
- používat více "specializovaných" e-mailových adres - např. pracovní email, email pro komunikaci s přáteli atd.
- jednou za čas změnit emailovou adresu
- používat antispamové řešení

5.2.1 Reklamy

Reklama na Internetu patří mezi nejrychleji se šířící formy reklamy. Nabídky zasílané prostřednictvím emailu jsou jednou z forem internetové reklamy. Jejich hlavní výhodou jsou téměř nulové náklady, velmi vysoká adresnost, okamžité doručení odkazu adresátovi a vysoká výnosnost. Společnosti se snaží tímto způsobem udržovat kontakt se svými stávajícími zákazníky, případně získávat nové.

Reklama zasílaná e-mailem je sama o sobě legitimní. Uživatel může mít zájem získávat reklamní informace z určité oblasti. Často si však nepřeje, aby mu reklama byla zasílána, ale přesto se tak děje. V takovém případě se reklamní email stává zároveň nevyžádanou poštou - spamem.

V současné době se množství nevyžádaných reklamních e-mailů stalo velkým problémem. Tvůrci nevyžádané pošty se přirozeně snaží vytvořit zdání legitimity; jednak legitimní reklama zasílaná ve velkých objemech vyvolává u uživatelů negativní reakci.

5.2.2 Fámy

Fáma (z anglického "hoax") je Internetem masově šířena zpráva. Nejčastějším médiem je elektronická pošta, případně komunikační nástroje typu ICQ a Skype. Jde buď o falešnou poplašnou zprávu, žert, nebo mystifikaci - zpráva sama o sobě se nezakládá na pravdě.

Mezi často rozšířené fámy patří například informace o novém počítačovém viru, který má běžné (mazání souborů, získávání hesel), nebo až přímo absurdně znějící schopnosti.

Některé poplašné zprávy útočí na city uživatelů. Autoři se snaží zajistit si co největší rozšíření zprávy výzvami na další přeposlání pod různými záminkami. Časté jsou fámy o mobilních telefonech, prosby o pomoc, nabídky na velké částky peněz ze zahraničí.

Ve většině případů je obtížné zjistit původní záměr autora.Možná stačí jen vědomí, že jeho zpráva bude šířit světem. V zásadě platí pravidlo, že pokud zpráva obsahuje výzvu k další hromadné rozesílání, je to s největší pravděpodobností fáma. Na Internetu existuje několik specializovaných stránek, které si budují databázi fám

(hoax).

5.2.3 Phishing

Pojem phishing se definuje kriminální činnost využívající tzv. sociální inženýrství (manipulační techniky vedoucí k získávání důvěrných informací). Cílem je získat citlivé údaje, jako například hesla k bankovním účtům, PIN kódy a jiné detaily.

Phishingem označujeme falešný email, tvářící se důvěryhodně, který se snaží vzbudit dojem, že jeho odesílatelem je např. banka nebo pojišťovna. Grafický vzhled zprávy, nebo stránka, na kterou zpráva odkazuje, je na první pohled nerozeznatelná od používaných stávajícími institucemi. Pod různými záminkami, například ověření přístupových údajů, zaslání částky peněz na účet, atd. jsou od uživatelů získány důvěrné informace. Ty mohou být později zneužity v neprospěch poškozeného.

Nejlepší obranou proti phishingu je něj vůbec neodpovídat.

5.2.4 Rozeznání nevyžádané pošty

Existuje několik znaků, podle kterých se dá rozpoznat, zda je emailová zpráva ve Vaší schránce nevyžádanou poštou. Pokud daná zpráva splňuje některou z následujících podmínek, jde pravděpodobně o nevyžádanou poštu - spam.

- adresa odesílatele nepatří do vašeho seznamu kontaktů
- dostanete výhodnou finanční nabídku, ale žádá se od Vás vstupní poplatek
- pod různými záminkami (ověření údajů, přesun financí) jsou od vás požadovány citlivé přístupové údaje (např. číslo bankovního účtu, heslo do Internetového bankovnictví)
- zpráva je napsána v cizím jazyce
- zpráva nabízí produkt, o který se nezajímáte. Pokud máte přece jen o produkt zájem, je vhodné si ověřit přímo u výrobce, zda odesílatel zprávy patří mezi důvěryhodné distributory
- zpráva obsahuje zkomolená slova, aby oklamala filtry pro nevyžádanou poštu. Například místo "viagra" bude "vaigra " a podobně

5.2.4.1 Pravidla

Pravidlo v antispamovém programu, případně poštovním klientu je účinným nástrojem pro manipulaci s poštou. Pravidlo se skládá ze dvou logických částí:

1) Podmínka (např. příchod zprávy z určité adresy)

2) Akce (např. smazání zprávy nebo přesunutí do předem určené složky)

Množství a variabilita pravidel závisí od-kterého konkrétního programu. Jejich funkcí je třídění pošty do logických celků a její administrace. Mohou zároveň sloužit i jako opatření proti nevyžádané poště. Typické příklady:

- Podmínka: Přijde zpráva obsahující slovo typické pro nevyžádanou poštu 2. akce: Smazat zprávu
- Podmínka: Příchozí zpráva obsahuje jako přílohu soubor s příponou. exe 2. akce: Smazat přílohu a zprávu uložit do schránky
- Podmínka: Přijde zpráva z domény zaměstnavatele 2. akce: zařaď zprávu do záložky "Pracovní"

Používání různých pravidel je běžnou součástí práce s programem a při vhodném nastavení pomáhá efektivně filtrovat nevyžádanou poštu.

5.2.4.2 Bayesiánsky filtr

Jde o velmi účinný způsob filtrování nevyžádané pošty, který je využíván většinou antispamových programů. Dokáže s vysokou přesností rozlišit, zda je daná zpráva nevyžádaná či nikoliv. Navíc se dokáže průběžně přizpůsobovat potřebám uživatele.

Princip fungování je následující: V první fázi probíhá proces "učení". Uživatel musí označit dostatečné množství zpráv za vyžádané a nevyžádané (například 200/ 200). Filtr se na základě analýzy výsledků naučí, že v nevyžádané poště - spamech se například často vyskytuje slovo "rolex" nebo "viagra" a v běžných zprávách se vyskytují jména příbuzných a známých. Pokud tedy prošlo analýzou vyšší množství zpráv, bayesiánský filtr dokáže podle výskytu slov přidělit "spamový index" a velmi přesně určit, zda jde o spam.

Hlavní výhodou je vysoká flexibilita. Pokud například uživatel v oblasti ekologie, tak všechny emaily s ekologickou tématikou budou mít přidělenu nižší pravděpodobnost spamu. Pokud zpráva obsahuje slovo/ slova, která by ji jinak zařadili mezi nevyžádanou poštu, ale odesílatelem je někdo z kontaktů, tak vyšší prioritu bude mít v tomto případě odesílatel zprávy. Zpráva ve výsledku nebude jako nevyžádaná pošta - spam.

5.2.4.3 Whitelist

Whitelist (v překladu "bílý seznam") je obecně seznam položek, případně osob, které jsou akceptovány, nebo mají někam zajištěn přístup. Pojmem emailový whitelist se označuje seznam kontaktů, které mají povolení doručovat zprávy do schránky. Seznamy lze vytvářet na základě klíčových slov, které jsou pak vyhledávány v emailových adresách, názvech domén, nebo v IP adresách.

Pokud je whitelist nastaven do režimu exkluzivity, zprávy z jiných adres, domén nebo IP adres se do pošty nedostanou. Pokud se whitelist sice používá, ne však v režimu exkluzivity, tak nevyžádaná pošta se obvykle přesune do schránky s nevyžádanou poštou.

Whitelist je založen na opačném principu než blacklist 115. Výhodou whitelistu je, že není tak náročný na údržbu jako blacklist. Obě metody lze vhodně zkombinovat a dosáhnout tak účinného filtrování nevyžádané pošty.

5.2.4.4 Blacklist

Blacklist ("černý seznam"), obecně seznam nebo zakázaných položek/ osob představuje ve virtuálním světě mechanismus, který povoluje přijímání elektronické pošty od všech odesílatelů, kteří se na blacklistu nenacházejí.

Blacklisty se vyskytují na dvou úrovních. Uživatel si sám ve antispamovém programu může definovat vlastní seznam. Existuje však možnost používat pravidelně aktualizovány, blacklisty od různých institucí, kterých se na Internetu nachází velké množství.

Blacklist pracuje v podstatě na opačném principu než whitelist 115. Jeho používání má velký význam pro blokování elektronické pošty. Je však náročný na údržbu, protože nové adresy, které je potebné přidat do seznamu, se zjevují neustále. Vhodnou a blacklistu se dá docílit efektivní filtrování nevyžádané pošty.

5.2.4.5 Kontrola na serveru

Kontrola na serveru je technika odhalování hromadných nevyžádaných zpráv na základě jejich počtu a uživatelské reakce. Na základě obsahu hlavní části zprávy se vypočítá digitální otisk "; číselná hodnota, která nedává žádnou informaci o zprávě, kromě toho, že dvě stejné zprávy budou mít stejný otisk, zatímco dvě různé zprávy budou mít téměř jistě otisk různý.

Pokud uživatel označí danou zprávu jako nevyžádanou poštu, odešle se na server její otisk po určitém počtu odeslání stejného otisku server uloží do své databáze otisků nevyžádané pošty. Při kontrole došlé pošty zase program posílá na server otisky přijatých zpráv, a server vrátí informaci, které otisky odpovídají poště, kterou jiní uživatelé označili jako "nevyžádanou".