ESET Mail Security 4

for Microsoft Exchange Server

Version 4.2

Používateľská príručka

Microsoft® Windows® 2000 / 2003 / 2008

ESET Mail Security

REV. 11/2/2010

Obsah

1. Úvod

ESET Mail Security 4 pre Microsoft Exchange Server je integrovaným riešením, ktoré chráni poštové schránky používateľov pred rôznymi typmi škodlivého obsahu (najčastejšie sú to prílohy e-mailových správ infikované červami alebo trojanmi, dokumenty obsahujúce škodlivé skripty, phishing, spam, atď.). ESET Mail Security poskytuje tri typy ochrany: Antivirus, Antispam a aplikáciu používateľských pravidiel. ESET Mail Security filtruje škodlivý obsah na úrovni poštového servera, skôr ako sa dostane do schránok klientov - príjemcov e-mailu.

ESET Mail Security podporuje verzie Microsoft Exchange Server versions 5.5 a novšie, ako aj Microsoft Exchange Server v prostredí klastrov (cluster environment). V novších verziách Microsoft Exchange Server (2007 a novšie) sú podporované aj špecifické role (mailbox, hub, edge). ESET Mail Security sa dá tiež vzdialene spravovať pomocou ESET Remote Administrator.

Čo sa týka funkcionality, ESET Mail Security je veľmi podobný produktu ESET NOD32 Antivirus 4.0. Obsahuje všetky nástroje potrebné pre zabezpečenie ochrany serveru ako klienta (rezidentná ochrana, ochrana prístupu na web, ochrana e-mailových klientov a antispam) a navyše poskytuje aj ochranu pre Microsoft Exchange Server.

1.1 Systémové požiadavky

Podporované operačné systémy:

- Microsoft Windows Server 2000
- 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
- Microsoft Windows Small Business Server 2003 R2
- Microsoft Windows Small Business Server 2008

Podporované verzie 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
- Microsoft Exchange Server 2010 SP1

Nároky na hardvér závisia od použitej verzie Microsoft Exchange Server a tiež od nainštalovaného operačného systému. Odporúčame prečítať si dokumentáciu k produktu Microsoft Exchange Server v prípade, že potrebujete detailné informácie o nárokoch na hardvér.

1.2 Metódy ochrany

Na kontrolu e-mailov sa používajú dve nezávislé metódy:

Kontrola poštových schránok cez VSAPI 3
Filtrovanie správ na úrovni SMTP servera 4

1.2.1 Kontrola poštových schránok cez VSAPI

Kontrola poštových schránok je spúšťaná a kontrolovaná Microsoft Exchange Serverom. Pošta v Microsoft Exchange Server store databáze sa kontroluje priebežne. V závislosti od verzie Microsoft Exchange Server (a náväzne aj verzie rozhrania VSAPI) a tiež od používateľských nastavení, môže byť kontrola spustená v ktorejkoľvek z týchto situácií:

- Keď používateľ pristupuje k e-mailu, napr. cez poštový program (pošta vždy prejde antivírusovou kontrolou s aktuálnou vírusovovou databázou)
- Na pozadí, ak je momentálne vyťaženie Microsoft Exchange Servera nízke.
- Proaktívne (závisí od vnútorného algoritmu Microsoft Exchange Servera)

Rozhranie VSAPI sa v súčasnosti využíva na antivírusovú kontrolu a ochranu použitím pravidiel.

1.2.2 Filtrovanie správ na úrovni SMTP servera

Filtrovanie na úrovni SMTP servera zabepečuje špecializovaný plugin. V Microsoft Exchange Server 2000 a Microsoft Exchange Server 2003 je to plugin (*Event Sink*) registrovaný na SMTP serveri ako súčasť Internet Information Services (IIS). V prípade verzií Micrososft Exchange Server 2007/2010 je plugin registrovaný ako transportný agent na Microsoft Exchange Server v roli *Edge* alebo *Hub*.

Filtrovanie SMTP na úrovni servera transportným agentom poskytuje antivírusovú, antispamovú ochranu a ochranu pomocou pravidiel, ktoré nastaví sám používateľ. Na rozdiel od VSAPI filtrovania, filtrovanie SMTP na úrovni servera prebieha predtým než sa kontrolovaná pošta doručí do mailového úložiska Microsoft Exchange Server (store).

1.3 Typy ochrany

Používajú sa tri hlavné typy ochrany:

1.3.1 Antivírusová ochrana

Antivírusová ochrana je jednou zo základných funkcií ESET Mail Security. Chráni používateľov proti útokom tak, že kontroluje súbory, emaily a internetovú komunikáciu. Ak je nájdená hrozba so škodlivým kódom, antivírusový modul ju odstráni tak, že ju najprv zablokuje a potom lieči/vymaže alebo presunie do karantény.

1.3.2 Antispamová ochrana

Antispamová ochrana integruje viacero technológií (RBL, DNSBL, Fingerprinting, Reputation checking, Content analysis, Bayesian filtering, Manual whitelisting/blacklisting, aplikácia pravidiel, atď.) pre dosiahnutie maximálnej presnosti detekcie. Výstupom z antispamového skenovacieho jadra je percentuálne vyjadrenie pravdepodobnosti že daný mail je SPAM (0 až 100). Pre účely EMSX sú hodnoty nad 90 vrátane považované za dostatočné pre klasifikovanie mailu ako SPAM.

Súčasťou antispamovej ochrany je aj technika Greylisting (štandardne je vypnutá). Vychádza zo špecifikácie RFC 821, podľa ktorej je SMTP protokol považovaný za nespoľahlivý, a preto v prípade dočasného zlyhania pri pokuse doručiť mail by sa ho mal každý mailový agent pokúsiť doručiť opakovane. Podstatná časť spamu je naopak doručovaná jednorázovo (špeciálnymi nástrojmi) a na množstvo adries získaných často automaticky "slovníkovým" spôsobom. Poštový server používajúci techniku Greylisting preto pre každú správu vypočíta kontrolnú sumu (hash) pre trojicu odosielateľ, príjemca a IP adresa odosielajúceho MTA. Ak server vo svojej databáze ešte takúto kontrolnú sumu nemá, správu odmietne prijať a vráti kód dočasnej chyby (temporary failure, napr. 451). Legitímny odosielajúci server sa po istom čase pokúsi správu doručiť opakovane a kontrolná suma sa pre danú trojicu zapíše do databázy overených spojení, čo zaručí, že prichádzajúce maily s touto charakteristikou sú už doručované okamžite.

1.3.3 Uplatňovanie používateľských pravidiel

Ochrana pomocou používateľských pravidiel je dostupná pri skenovaní pomocou VSAPI aj pri skenovaní transportným agentom. Používateľ môže zadávať pravidlá, ktoré sa dajú navzájom kombinovať. Zadaním viacerých podmienok v rámci jedného pravidla budú tieto prepojené pomocou logického operátora AND, čo znamená, že pravidlo bude vykonané len vtedy, ak budú splnené všetky jeho podmienky. Zadaním viacerých samostatných pravidiel sa medzi nimi aplikuje logický operátor OR, čo znamená, že sa vykoná prvé pravidlo, ktorého podmienky sú splnené.

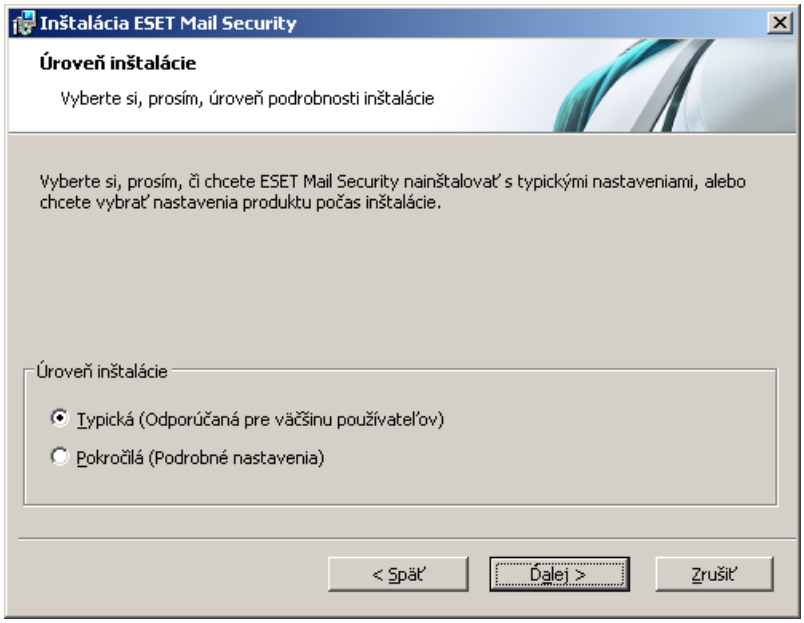
V procese kontroly je prvou použitou technikou greylisting - ak je povolená. Ďalej v poradí nasleduje ochrana pomocou používateľských pravidiel, antivírusová kontrola a nakoniec antispamová kontrola.

2. Inštalácia

Program ESET Mail Security je možné po zakúpení nainštalovať z inštalačného CD-ROM média, ktoré je súčasťou produktového balenia, alebo je možné inštalačný súbor prevziať priamo zo stránky www.eset.sk v podobe inštalačného balíčka .msi.

Po jeho spustení Vám s inštaláciou bude pomáhať sprievodca, ktorý vás prevedie základnými nastaveniami. Na výber sú 2 typy inštalácie s rôznymi úrovňami podrobnosti nastavení:

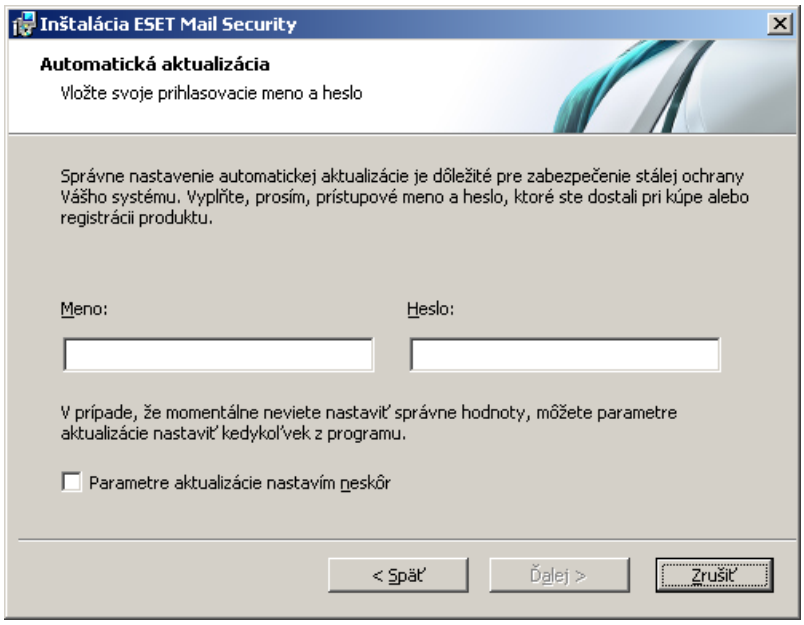
1. **Typická inštalácia**
2. **Pokročilá inštalácia**



2.1 Typická inštalácia

Je odporúčaná pre užívateľov, ktorí chcú ESET Mail Security nainštalovať s typickými nastaveniami. Typické nastavenia programu poskytujú maximálny stupeň ochrany, čo ocenia najmä menej skúsení užívatelia, ktorí nemajú potrebu prechádzať podrobnými nastaveniami.

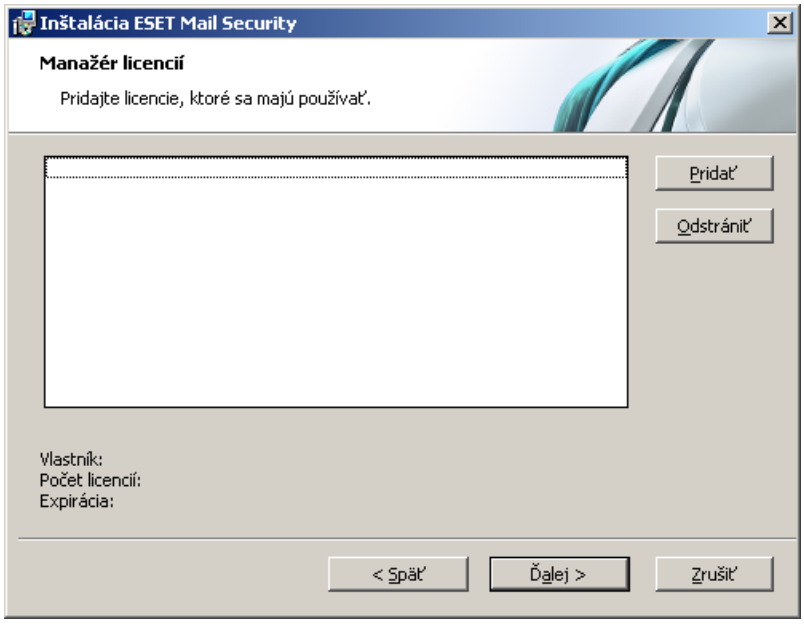
Prvým, veľmi dôležitým krokom inštalácie je **nastavenie prihlasovacieho mena a hesla** pre automatickú aktualizáciu programu. Tá zohráva podstatnú úlohu pri zabezpečovaní stálej ochrany počítača.



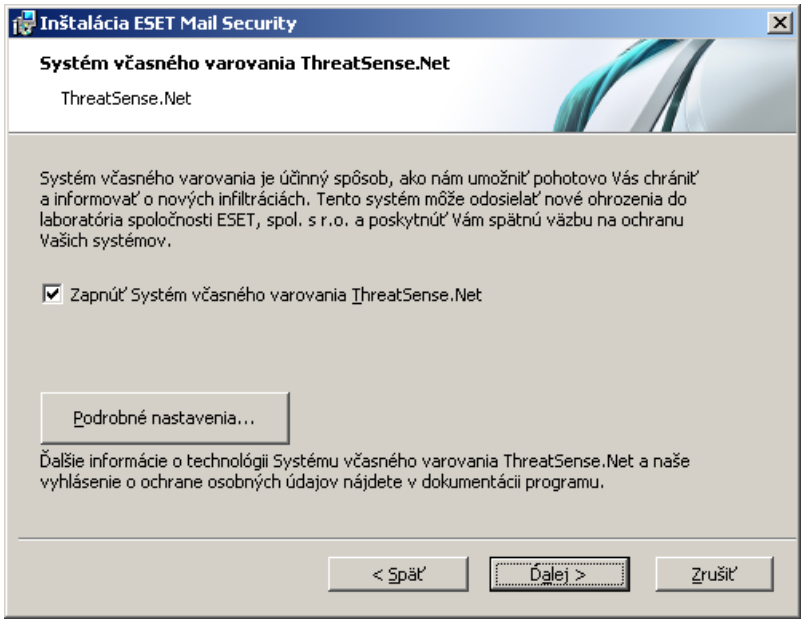
Do položiek Meno a Heslo je potrebné vyplniť prihlasovacie údaje, ktoré ste získali pri kúpe alebo registrácii produktu. Ak momentálne tieto údaje neviete, označte zaškrtávací rámček Parametre aktualizácie nastavím neskôr. Prihlasovacie

údaje môžete nastaviť kedykoľvek priamo z programu.

V ďalšom kroku v okne **Manažér licencií** pridajte stlačením **Pridať** licenciu, ktorá Vám bola doručená v e-mailovej správe po kúpe produktu.



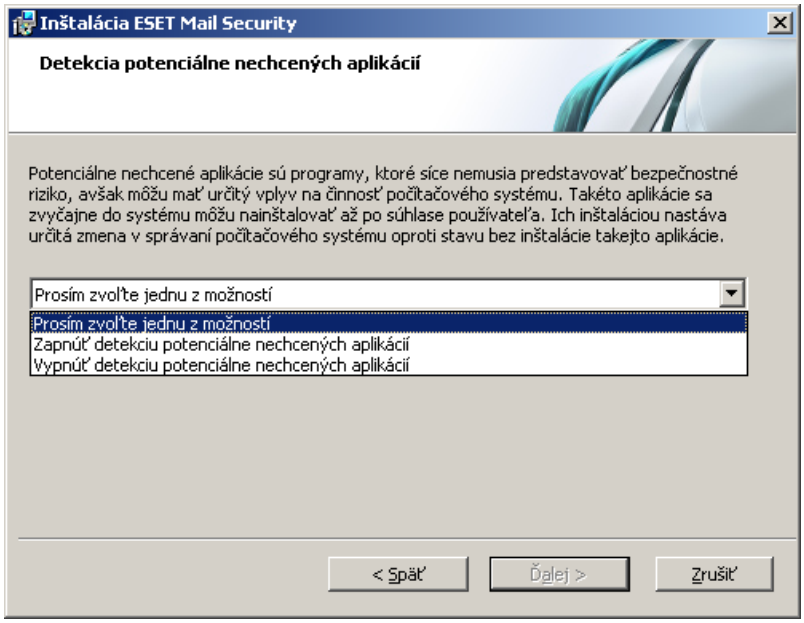
Ďalším krokom inštalácie je nastavenie systému včasného varovania ThreatSense.Net, ktorý umožňuje, aby spoločnosť ESET, spol. s r. o. bola pohotovo a neustále informovaná o nových infiltráciách, a tak efektívne chránila svojich zákazníkov. Systém dovoľuje odosielať nové druhy hrozieb do vírusového laboratória spoločnosti ESET, spol. s r. o., kde sú tieto hrozby analyzované a zapracovávané do vírusových databáz.



Označením zaškrtávacieho rámčeka **Zapnúť Systém včasného varovania ThreatSense.Net** tento systém aktivujete. V podrobných nastaveniach (po stlačení tlačidla **Podrobné nastavenia**) máte možnosť ovplyvniť detaily posielania podozrivých súborov.

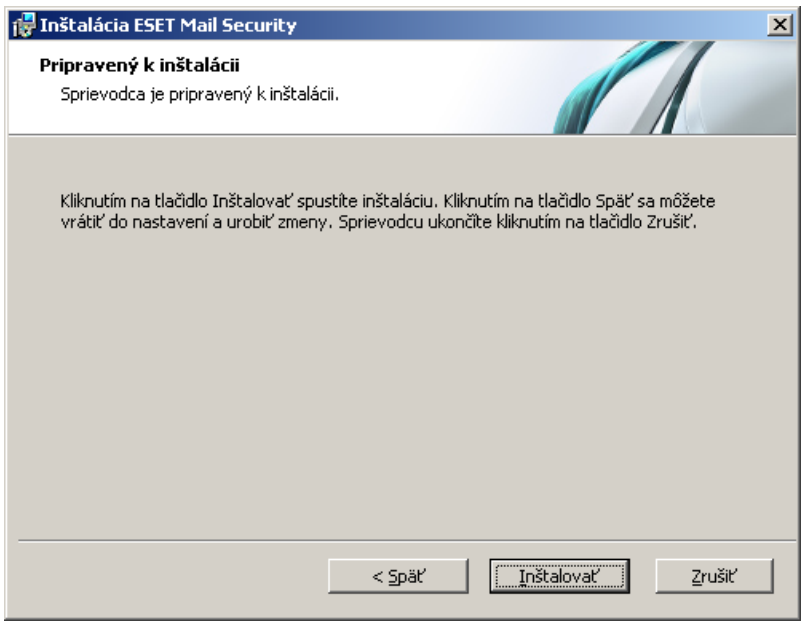
Ďalším inštalačným krokom je **nastavenie možnosti detekcie potenciálne nechcených aplikácií**. Potenciálne nechcené aplikácie predstavujú programy, ktoré nie vždy priamo predstavujú bezpečnostné riziko, môžu mať však vplyv na korektné fungovanie operačného systému. Obvykle sú tieto aplikácie inštalované po súhlase užívateľa.

To je možné vďaka tomu, že bývajú súčasťou inštalácie iných programov a súhlas k inštalácii môže užívateľ ľahko prehliadnuť. Inštaláciou potenciálne nechcených aplikácií zvyčajne nastáva zmena v správaní operačného systému, v porovnaní so stavom bez inštalácie takejto aplikácie.



Označením voľby Zapnúť detekciu potenciálne nechcených aplikácií povolíte, aby ESET Mail Security detegoval aj tento typ hrozieb. Odporúčame, aby ste detekciu týchto aplikácií povolili.

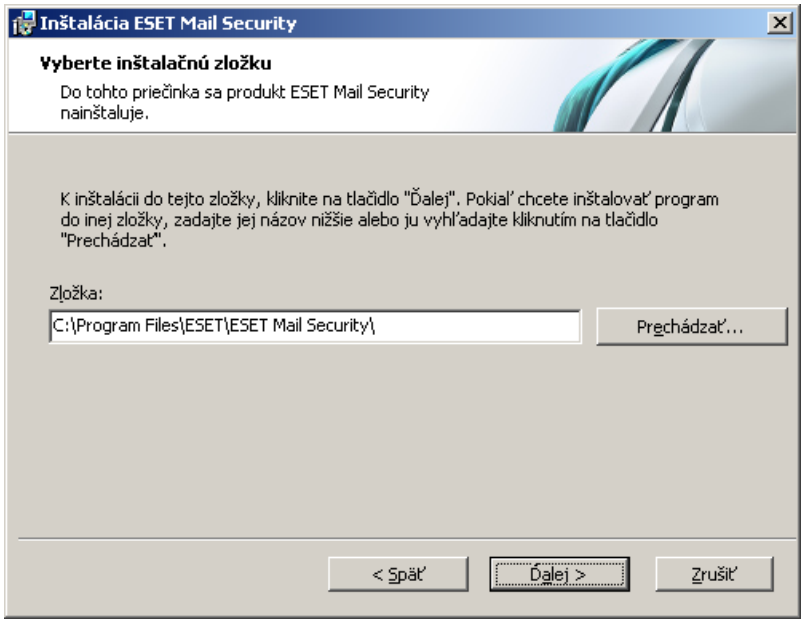
Posledným krokom typickej inštalácie je potvrdenie inštalácie programu kliknutím na tlačidlo **Inštalovať**.



2.2 Pokročilá inštalácia

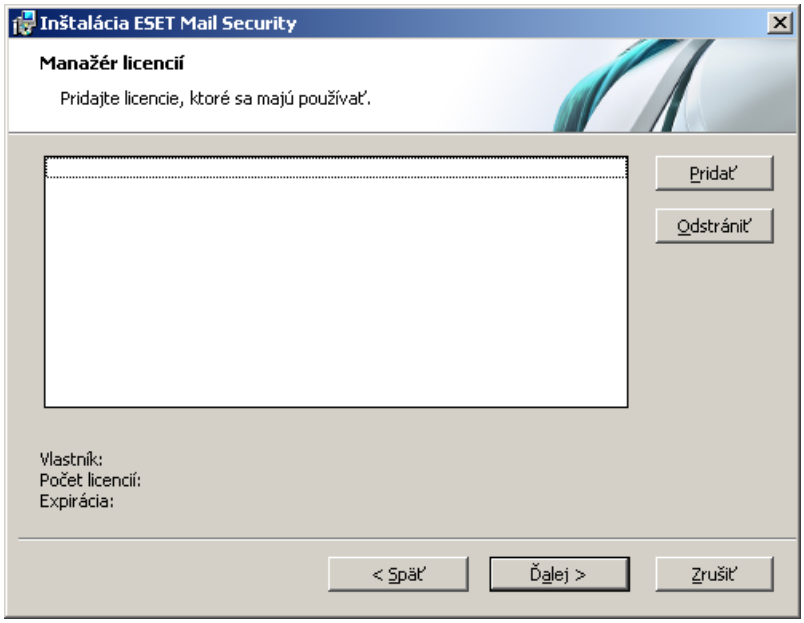
Je určená pre užívateľov, ktorí majú skúsenosti s nastavovaním programov a pri inštalácii programov zvyknú meniť pokročilé nastavenia. Prvým krokom je nastavenie umiestnenia programu.

Štandardne sa program inštaluje do adresára
C:\Program Files\ESET\ESET Mail Security.
Umiestnenie je možné zmeniť prostredníctvom tlačidla **Prechádzať...**

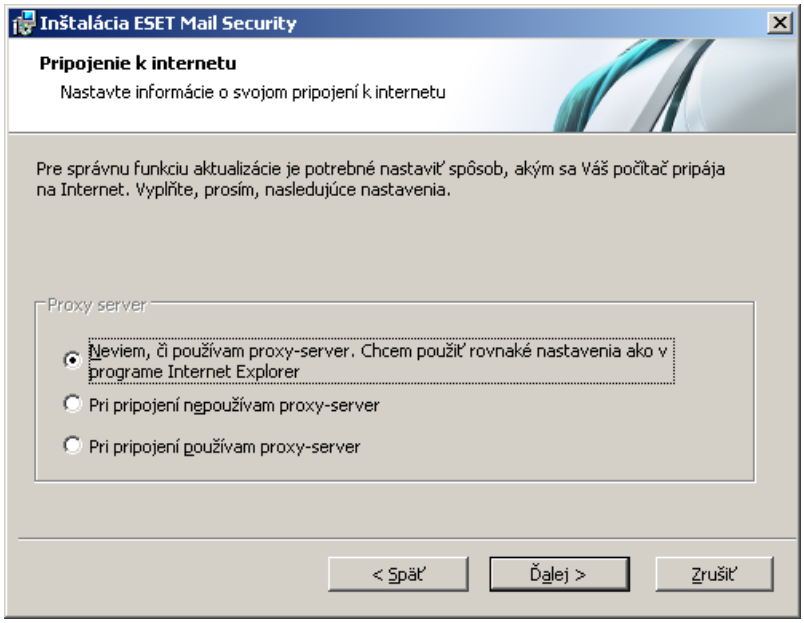


Nasledujúcim krokom je nastavenie prihlasovacieho mena a hesla. Tento krok je rovnaký ako pri Typickej inštalácii 5.

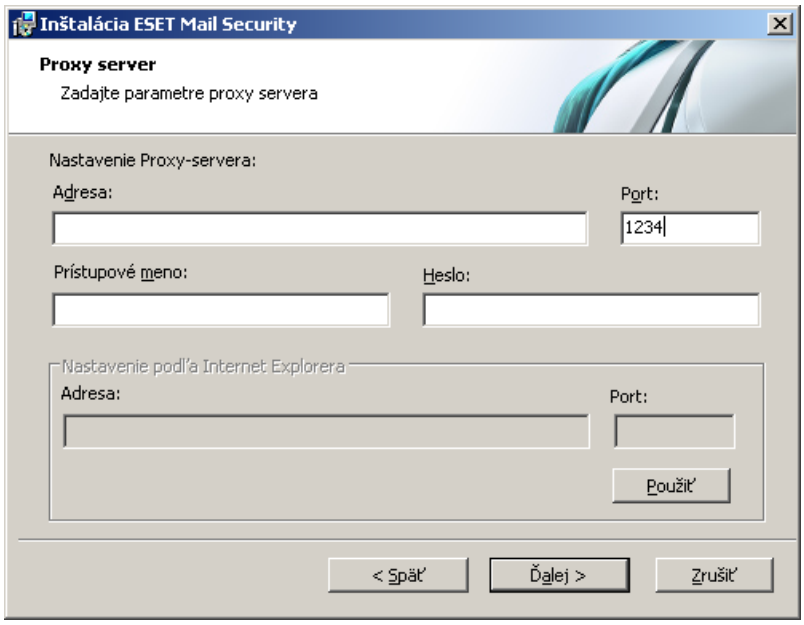
V ďalšom kroku v okne **Manažér licencií** pridajte stlačením **Pridať** licenciu, ktorá Vám bola doručená v e-mailovej správe po kúpe produktu.



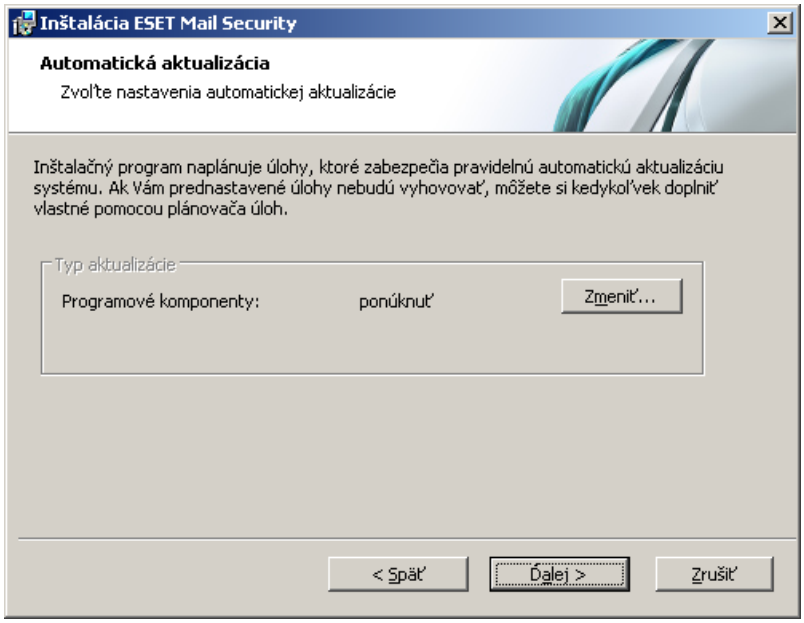
Nasleduje nastavenie spôsobu pripojenia na Internet. Ak ku pripojeniu na internet používate telefónnu linku, označte možnosť **Na internet sa pripájam pomocou telefónnej linky**. V opačnom prípade ponechajte možnosť neoznačenú.



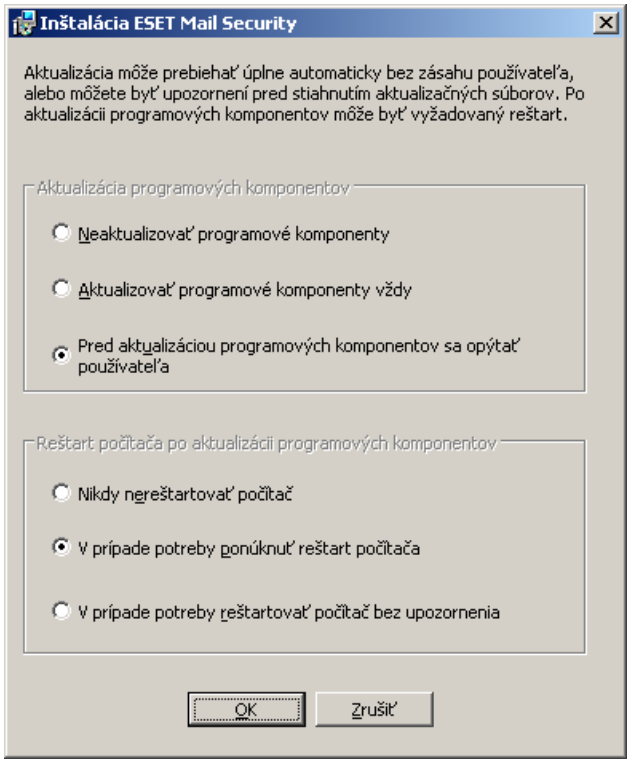
Nastavenia proxy servera sú dôležité pre správne fungovanie aktualizácie programu. V prípade, že neviete, či pri pripojení na internet používate proxy-server, označte možnosť **Neviem, či používam proxy-server** a kliknine na **Ďalej** ; nastavenie sa prevezme z nastavení Internet Explorera. Ak proxy server nepoužívate, označte príslušnú možnosť.



Ak pri pripojení proxy-server používate a vybrali ste túto možnosť, v ďalšom kroku Vás inštalátor požiada o upresnenie nastavení proxy-servera. Do políčka **Adresa** vpíšte IP adresu alebo URL proxy servera. Pole **Port** slúži na určenie portu, na ktorom proxy-server prijíma spojenie (štandardne 3128). Ak proxy-server vyžaduje autentifikáciu, je potrebné vyplniť polia **Prístupové meno** a **Heslo**. Proxy-server môžete nastaviť aj podľa nastavení Internet Explorera. Ak si želáte nastaviť proxy-sever týmto spôsobom, kliknite na tlačidlo **Použiť** a potvrďte okno s výzvou.

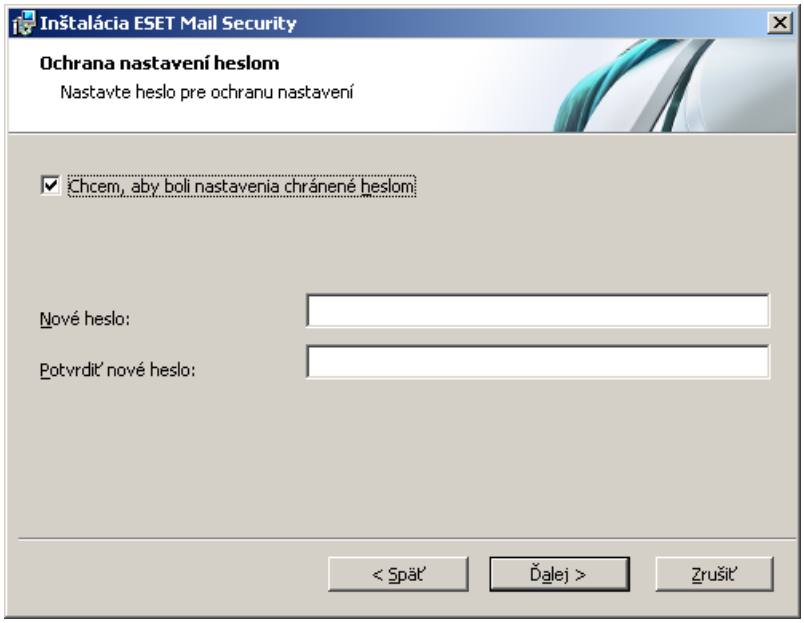


Nasledujúcim krokom inštalácie je nastavenie automatickej aktualizácie programových komponentov ESET Mail Security alebo, inými slovami, automatický upgrade programu na novú verziu. Pomocou tlačidla **Zmeniť** vstúpite do podrobnejších nastavení. Ak si neželáte, aby boli programové komponenty aktualizované automaticky, zvoľte **Neaktualizovať programové komponenty**. Voľbou **Upozorniť pred aktualizáciou programových komponentov** si vyžiadate potvrdenie stiahnutia a inštalácie programových komponentov. Automatickú aktualizáciu programových komponentov zabezpečíte voľbou **Aktualizáciu programových komponentov vykonať vždy, keď je k dispozícii**.



Poznámka: Po aktualizácii programových komponentov je obvykle vyžadovaný reštart počítača. Preto odporúčame nastavenie **V prípade potreby ponúknuť reštart počítača.**

Ďalším krokom inštalácie je nastavenie hesla pre ochranu nastavení programu. Zvoľte heslo, ktoré bude vyžadované pri každej zmene alebo prístupe k nastaveniam ESET Mail Security. Pre potvrdenie hesla musíte napísať heslo znova, predíde sa tak možnému preklepu.



Kroky inštalácie pre nastavenie **ThreatSense.Net** a **detekcie potenciálne nechcených aplikácií** sú rovnaké ako pri Typickej inštalácii 5.

Posledným krokom pokročilej inštalácie je potvrdenie inštalácie programu kliknutím na tlačidlo **Inštalovať**.

2.3 Aktualizácia na novšiu verziu

Novšie verzie ESET Mail Security sú vydávané za účelom zdokonalenia produktu a opravy chýb, ktoré nie je možné opraviť v rámci automatickej aktualizácie programových modulov. Je niekoľko spôsobov ako aktualizovať produkt na novšiu verziu:

1. Automaticky prostredníctvom aktualizácie programových komponentov (PCU)
   Keďže aktualizácia programových komponentov sa týka všetkých používateľov daného produktu a môže mať významný dopad na systém, je vydávaná až po dlhom období testovania na všetkých operačných systémoch v rôznych konfiguráciách. Ak potrebujete aktualizovať na najnovšiu hneď po jej vydaní, použitie niektorú z nasledujúcich dvoch metód.

2. Manuálne - stiahnutím z webu a preinštalovaním staršej verzie.
   Na začiatku preinštalácie je možné zvoliť zachovanie aktuálnych nastavení programu (voľba **Použiť pôvodné nastavenia**).

3. Manuálne s automatickou vzdialenou inštaláciou na stanice v sieti prostredníctvom ESET Remote Administrator.

2.4 Inštalácia v prostredí clusterov

Cluster je skupina serverov (serveru zapojenému v clusteri sa hovorí „node" – „uzol"), ktoré fungujú spoločne ako jeden server. Takéto prostredie poskytuje vysokú dostupnosť a spoľahlivosť poskytovaných služieb. Ak jeden z uzlov v clusteri zlyhá alebo sa stane nedostupný, jeho funkciu automaticky preberie ďalší. ESET Mail Security plne podporuje MS Exchange Servery zapojené do clustera. Dôležité je, aby mal ESET Mail Security na všetkých uzloch v clustery stále rovnakú konfiguráciu. To je možné zabezpečiť prostredníctvom ESET Remote Administrator (použitím policy). V nasledujúcich častiach si ukážeme, ako nainštalovať a nakonfigurovať ESET Mail Security na uzly v clustery pomocou ESET Remote Administrator (ERA).

Inštalácia

V tejto kapitole je opísaná Push inštalácia, nie je to však jediný spôsob ako nainštalovať produkt na cieľový počítač. Podrobnejšie informácie nájdete v dokumentácii k ESET Remote Administrator.

1) Na počítač s ERA stiahnite msi inštalačný balík ESET Mail Security z webovej stránky ESETu. V ERA v záložke **Remote Install** v časti **Computers** kliknite pravým tlačítkom na ľubovoľné miesto do zoznamu počítačov a v kontextovom menu vyberte možnosť **Manage Packages**. V menu **Type** zvoľte **ESET Security Products package**, kliknite na **Add...** a ako **Source** vyberte stiahnutý msi inštalačný balík ESET Mail Security. Kliknite na **Create**.

2) V časti **Edit/Select configuration associated with this package** zvoľte **Edit** a nakonfigurujte nastavenia **ESET**

Mail Security podľa Vašich potrieb. V konfiguračnom editore sa nastavenia týkajúce sa ESET Mail Security nachádzajú vo vetve **ESET Smart Security**, **ESET NOD32 Antivirus** > **Mail server protection** a **Mail server protection for Microsoft Exchange Server**. Samozrejme, je možné nastaviť aj parametre ostatných modulov, ktoré ESET Mail Security obsahuje (napr. Update module, Computer scan, atď.). Nakonfigurované nastavenia odporúčame vyexportovať do xml súboru, ktorý je neskôr možné použiť napr. pri vytváraní inštalačného balíka (Installation Package), aplikovaní konfiguračnej úlohy (Configuration Task) alebo politiky (Policy).

3) Kliknite na **Close**, v dialógovom okne s otázkou **Do you want to save the package into server ?** zvoľte **Yes** a v nasledujúcom okne zvoľte názov inštalačného balíka. Inštalačný balíček sa pod zvoleným názvom a so zadefinovanou konfiguráciou uloží na server a je pripravený na použitie. Najčastejším je použitie priamo pri vzdialenej inštalácii (Push Install), ale je možné ho aj samostatne uložiť ako klasický msi inštalačný balík a použiť pri priamej inštalácií na serveri (voľba **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.

Poznámka: Pre bezproblémový priebeh vzdialenej inštalácie je potrebné splniť niekoľko podmienok ako na strane cieľovej stanice, tak i na strane ERA Servera. Podrobnejšie informácie nájdete v dokumentácii k ESET Remote Administrator.

Konfigurácia

Pre správne fungovanie ESET Mail Security na uzloch v clusteri je dôležité, aby boli stále rovnako nakonfigurované. Pokiaľ ste dodržali vyššie uvedený postup, je táto podmienka splnená. Stále však hrozí, že na jednom z uzlov bude táto konfigurácia omylom zmenená a dôjde tak k inkonzistencii nastavení medzi jednotlivými ESET Mail Security v clusteri. Tomuto sa dá vyhnúť použitím policy v ESET Remote Administrator. Policy sa v mnohom podobá na bežnú konfiguračnú úlohu (Configuration Task) – ide o vyslanie konfigurácie zadefinovanej v konfiguračnom editore (Configuration Editor) na klienta/klientov. V prípade policy však nejde o jednorázové vyslanie konfigurácie, ale o celkové zabezpečenie určitej konfigurácie spravovaných ESET security produktov. Policy by sme teda mohli zadefinovať ako konfiguráciu, ktorá je neustále vnucovaná klientovi / skupine klientov.

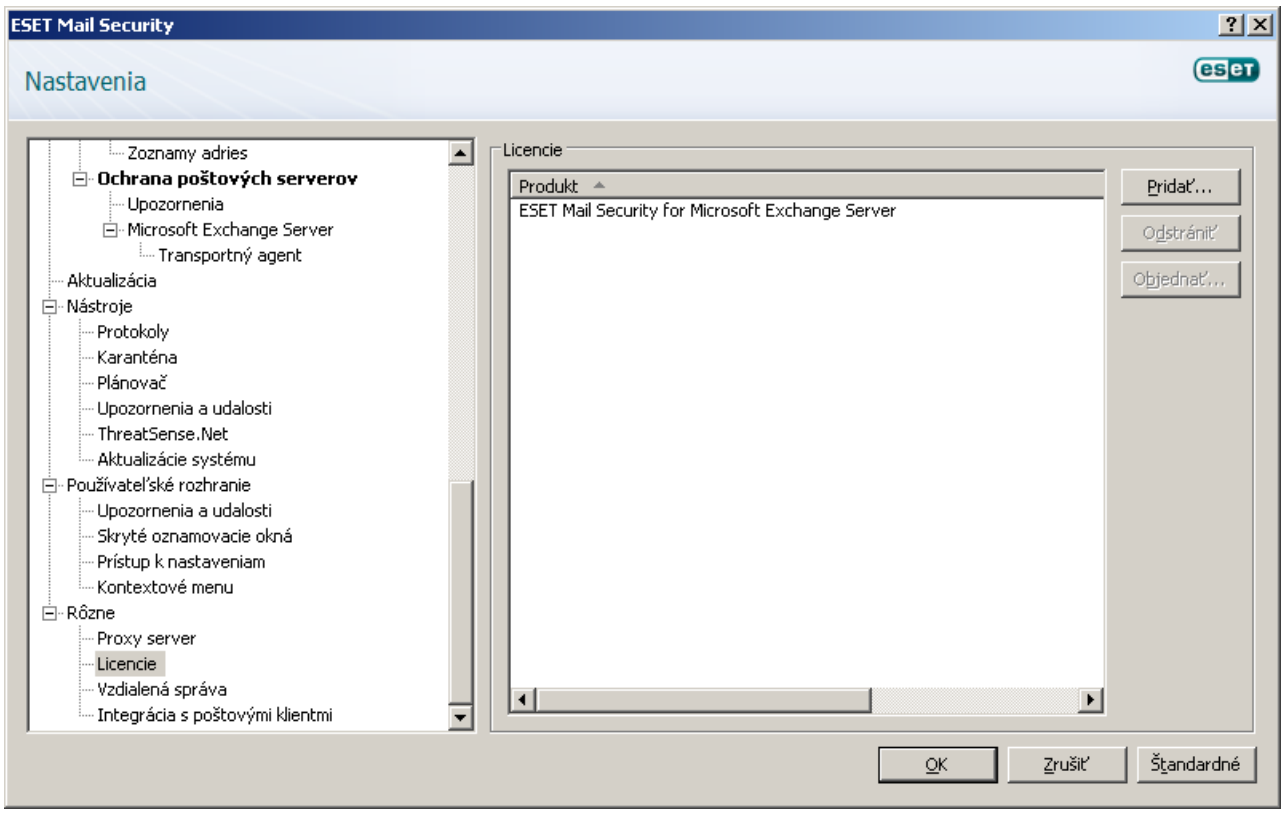
V **Tools** > **Policy Manager...** existuje niekoľko možností ako použiť policy. Najjednoduchšou možnosťou je využiť **Default Parent Policy**, ktorá štandardne slúži aj ako **Default policy for primary clients**. Táto policy má tú vlastnosť, že sa automaticky aplikuje na všetkých priamo pripojených klientov – t.j. v našom prípade na vzdialene nainštalované ESET Mail Security na uzloch v clusteri. Policy je možné nakonfigurovať po stlačení tlačidla **Edit...**, pričom je možné využiť už existujúcu konfiguráciu uloženú v xml súbore, ak sme si ju predtým vytvorili.
Druhou možnosťou je vytvoriť si novú policy (**Add New Child Policy**) a pomocou **Add Clients...** jej priradiť všetky ESET Mail Security na serveroch v clustery.

Táto konfigurácia zabezpečí, že na všetkých klientov budú prostredníctvom jednej policy aplikované rovnaké nastavenia. Ak v budúcnosti budeme chcieť zmeniť nastavenia v ESET Mail Security v clusteri, stačí zmeniť danú policy. Zmeny sa prenesú na všetkých klientov spadajúcich pod danú policy.

Poznámka: Podrobnejšie informácie k využitiu policies nájdete v dokumentácií k ESET Remote Administrator.

2.5 Licencia

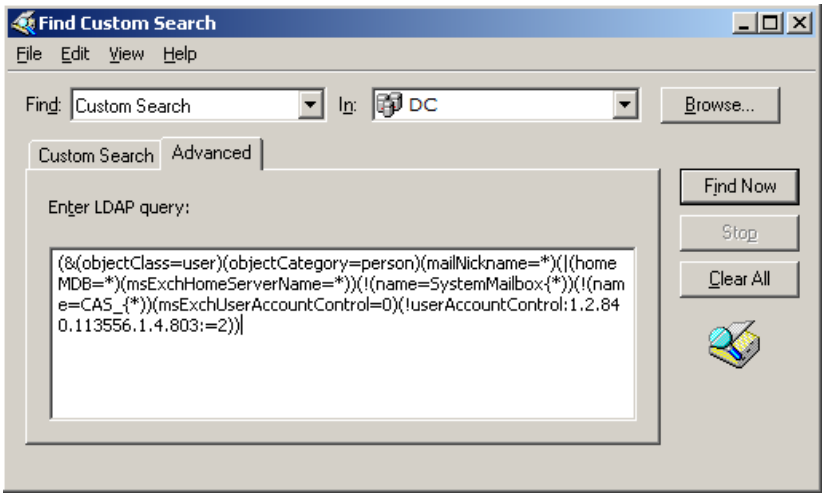
Veľmi dôležitý krok je vloženie licenčného súboru pre ESET Mail Security pre Microsoft Exchange Server. Bez licencie nebude ochrana pošty na systéme Microsoft Exchange Server fungovať správne. Ak nevložíte licenciu do produktu počas inštalácie, môžete tak urobiť neskôr v rozšírených nastaveniach v časti **Rôzne > Licencie.**



ESET Mail Security porovnáva počet poštových schránok v active directory s počtom poštových schránok definovaných v použitej licencii. Ak je v sústave napojených viac Exchange serverov, pri zisťovaní celkového počtu poštových schránok sa berú do úvahy aj active directory týchto Exchange serverov. Systémové poštové schránky, deaktivované poštové schránky a emailové aliasy sa do počtu použitých poštových schránok nezapočítavajú. V prostredí clustera sa uzly s rolou "clustered mailbox" do počtu použitých poštových schránok nezapočítavajú.

Počet použitých poštových schránok v MS Exchange je možné zistiť nasledovným spôsobom. Na serveri otvorte **Active Directory Users and Computers**. Pravým tlačítkom myši kliknite na doménu a v kontextovom menu zvoľte **Find...**.V roletovom menu **Find** menu zvoľte **Custom Search** a kliknite na záložku **Advanced**. Do textového poľa nakopírujte nasledovnú LDAP (Lightweight Directory Access Protocol) požiadavku a stlačte **Find Now**:

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



Ak počet poštových schránok v active directory prekročí počet poštových schránok definovaných v licencií, do logu Microsoft Exchange Servera sa zapíše hlásenie "Protection status changed due to exceeded number of mailboxes (count) covered by your license (count).". Zároveň sa v ESET Mail Security zmení **Stav ochrany** na **ORANŽOVÚ** a zobrazí sa správa informujúca o 42 dňovej lehote, po uplynutí ktorej bude ochrana vypnutá. V takomto prípade odporúčame kontaktovať predajcu a rozšíriť si licenciu o chýbajúci počet poštových schránok.

Ak počas 42 dňovej lehoty nebude vložená nová licencia pokrývajúca chýbajúce poštové schránky, **Stav ochrany** zmení farbu na **ČERVENÚ** a zobrazí sa správa o vypnutí ochrany z dôvodu prekročenia počtu poštových schránok. V takomto prípade odporúčame okamžite kontaktovať predajcu a zabezpečiť rozšírenie licencie o chýbajúci počet poštových schránok.

2.6 Nastavenia po inštalácii

Pre zabezpečenie optimálnej funkčnosti a maximálnej ochrany je potrebné po nainštalovaní produktu vhodne nakonfigurovať niektoré základné nastavenia.

Nastavenia Antispamu

Táto časť popisuje nastavenia, metódy a techniky, ktoré môžete použiť na ochranu Vašej siete pred spamom. Odporúčame Vám, aby ste si prečítali všetky nasledujúce inštrukcie skôr, ako si vyberiete tú najvhodnejšiu kombináciu nastavení pre Vašu sieť.

Spravovanie spamu

Pre optimálne fungovanie antispamovej ochrany je potrebné definovať, ako budú ďalej spracované správy vyhodnotené ako SPAM.

K dispozícii sú tieto tri možnosti:

1. **Vymazávanie spamu**

   Vzhľadom na to, že hranica na posúdenie správy ako SPAM je v ESET Mail Security nastavená bezpečne vysoko, je riziko zmazania legitímnej správy minimálne. Platí tu pravidlo, že čím podrobnejšie sú špecifikované nastavenia Antispamu, tým je menšia pravdepodobnosť, že bude vymazaná legitímna pošta. Medzi výhody tejto metódy patrí jej nenáročnosť na systémové prostriedky a menej času stráveného administráciou. Nevýhodou je, že ak aj dôjde k prípadnému zmazaniu legitímnej správy, nie je ju možné lokálne obnoviť.

2. **Karanténa**

   Táto možnosť vylučuje riziko vymazania legitímnej pošty. Správy sa dajú okamžite obnoviť a preposlať pôvodným príjemcom. Nevýhodami tejto metódy sú vyššie zaťaženie Microsoft Exchange Servera a dodatočný čas potrebný na údržbou e-mailovej karantény. Na presunutie mailu do karantény môžete využiť dva spôsoby:

   A. Interná karanténa Microsoft Exchange Servera:
   - ak chcete použiť internú karanténu servera uistite sa, že pole **Spoločná karanténa správ** v pravej časti okna menu rozšírených nastavení (**Ochrana poštových serverov > Spoločná karanténa správ**) je prázdne a aktivujte voľbu **Uložiť do systémovej karantény správ poštového servera** z roletového menu v spodnej časti.

   B. Vlastná poštová schránka karantény:
   - ak zadáte želanú adresu do poľa **Spoločná karanténa správ**, ESET Mail Security začne presúvať všetky nové správy do tejto Vami zadefinovanej e-mailovej schránky.

3. **Preposielanie spamu**

   Spam sa bude preposielať ďalej do organizácie, s tým, že ESET Mail Security do každej správy doplní príslušný MIME header s SCL hodnotou, na základe ktorej potom IMF (Intelligent Message Filtering) Exchange Servera vykoná príslušné akcie.

Filtrovanie spamu

Antispamové jadro
Antispamové jadro ponúka tri konfigurácie - **Odporúčaná, Maximálna presnosť, Maximálna rýchlosť.**
V prípade, že nie je nutné optimalizovať konfiguráciu na maximálnu priepustnosť (napr. pri zvýšenej záťaži servera), odporúčame vybrať konfiguráciu **Maximálna presnosť.** Pri konfigurácii **Odporúčaná** si antispamové jadro dolaďuje konfiguráciu automaticky na základe skenovaných správ. Ak je zapnutá možnosť **Maximálna presnosť** nastavenia sa optimalizujú s ohľadom na čo najspoľahlivejšiu detekciu. Extra výber **Vlastná > Otvoriť konfiguračný súbor** umožní používateľovi upraviť súbor spamcatcher.conf. Túto možnosť odporúčame len pre pokročilých používateľov.

Pred spustením plnej prevádzky servera Vám odporúčame nastaviť zoznamy blokovaných a povolených IP adries:

1) Otvorte okno rozšírených nastavení programu a v ňom sekciu **Antispamová ochrana > Ochrana poštových serverov.**
2) Označte pole **Povoliť antispamovú ochranu poštových serverov.**
3) Kliknite na tlačidlo **Nastaviť...** definujte **Povolené, Ignorované** a **Blokované IP adresy.**
   - V záložke **Blokované IP adresy** môžete pridávať IP adresy, ktoré by mali byť blokované, t.j. ak akákoľvek neignorovaná IP adresa v prijatých hlavičkách (Received headers) súhlasí s hociktorou adresou v tomto zozname, správe sa pridelí skóre 100 a už neprebiehajú žiadne ďalšie kontroly.
   - V záložke **Povolené IP adresy** môžete pridávať IP adresy, ktoré majú mať štatút povolené, t.j. ak prvá neignorovaná IP adresa v prijatých hlavičkách (Received headers) súhlasí s hociktorou adresou v tomto zozname, správe sa pridelí skóre 0 a viac sa už nekontroluje.
   - V záložke **Ignorované IP adresy** môžete pridávať IP adresy, ktoré budú ignorované počas RBL kontrolyl (*Real-time Blackhole List (RBL) checks*). V tomto zozname by sa mali nachádzať všetky interné IP adresy firewallu, ktoré nie sú priamo dostupné z Internetu. Pridaním takýchto adries zabránite nepotrebným kontrolám interných IP adries a umožníte systému identifikovať pripájajúce sa externé IP adresy.

Greylisting
Greylisting je metóda, ktorá chráni používateľov pred spamom pomocou nasledovnej techniky: Transportný agent posiela návratovú SMTP hodnotu *temporarily rejected* ('dočasne zamietnutá' = prednastavená je hodnota 451/4.7.1) na každú prijatú správu, ktorá nepochádza z identifikovaného zdroja. Legitímny odosielajúci server sa po istom čase pokúsi správu znovu doručiť. Spamové servery sa zvyčajne nepokúšajú tieto správy pri neuspešnom doručení znova odoslať, pretože odosielajú tísíce emailových adries naraz a nemajú čas na spätnú kontrolu.

Pri vyhodnocovaní zdroja správy sa berú do úvahy nastavenia na zoznamoch: **Povolené IP adresy**, **Ignorované IP adresy**, zoznamy **Safe Senders** a **Allow IP** definované na Exchange Serveri, a tiež nastavenie AntispamBypass pre daný mailbox. Greylisting je metóda, ktorá musí byť dôkladne nastavená, inak môže mať za následok nežiadúce efekty ako je pozdržanie doručenia správ z legitímnych zdrojov alebo od známych odosielateľov. Tento efekt bude postupom času ustupovať zároveň s tým, ako si bude metóda budovať interný whitelist overených spojení. V prípade, že vám daná metóda nie je známa, alebo spomenutý vedľajší efekt pre vás nie je pripustný, odporúčame metódu vypnúť v menu rozšírených nastavení pod **Antispamová > ochrana > Ochrana poštových serverov > Microsoft Exchange Server > Transportný agent > Povoliť techniku Greylisting.**

Rovnako doporučujeme metódu vypnúť, ak produkt používate len na otestovanie funkcionality a nechcete nastavovať rozšírené funkcionality programu.

Poznámka: Greylisting je len doplnkovou vrstvou ochrany pred spamom a nemá žiaden vplyv na hodnotiace schopnosti antispamového modulu.

Nastavenia antivírusovej ochrany

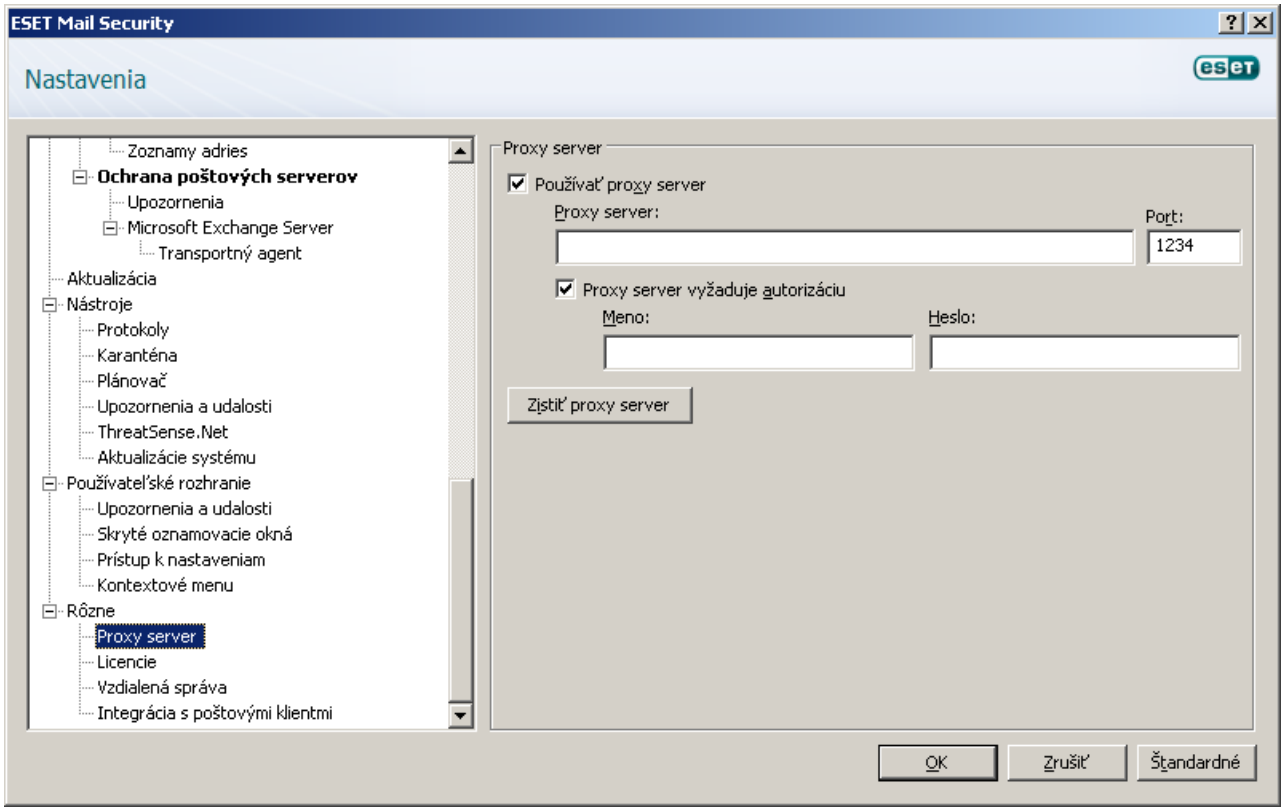
Karanténa
V závislosti od nastaveného režimu liečenia odporúčame definovať v nastaveniach akciu, ktorá bude aplikovaná na infikované (neliečené) správy. Túto možnosť nájdete v rozšírenom menu pod **Antivírus a antispyware > Ochrana poštových serverov > Microsoft Exchange Server > Transportný agent.**
Ak je možnosť posielať správy do mailovej karantény aktívna, je nevyhnutné definovať karanténu v menu rozšírených nastavení v sekcii **Karanténa správ.**

Výkon
Ak tomu nebránia iné obmedzenia, odporúčame Vám zvýšiť počet skenovacích jadier podľa vzorca: *počet skenovacích jadier = počet vlákien kontroly* a počet vlákien kontroly podľa vzorca: *(počet fyzických procesorov * 2) + 1* v menu rozšírených nastavení pod **Antivírus a antispyware > Výkon.**

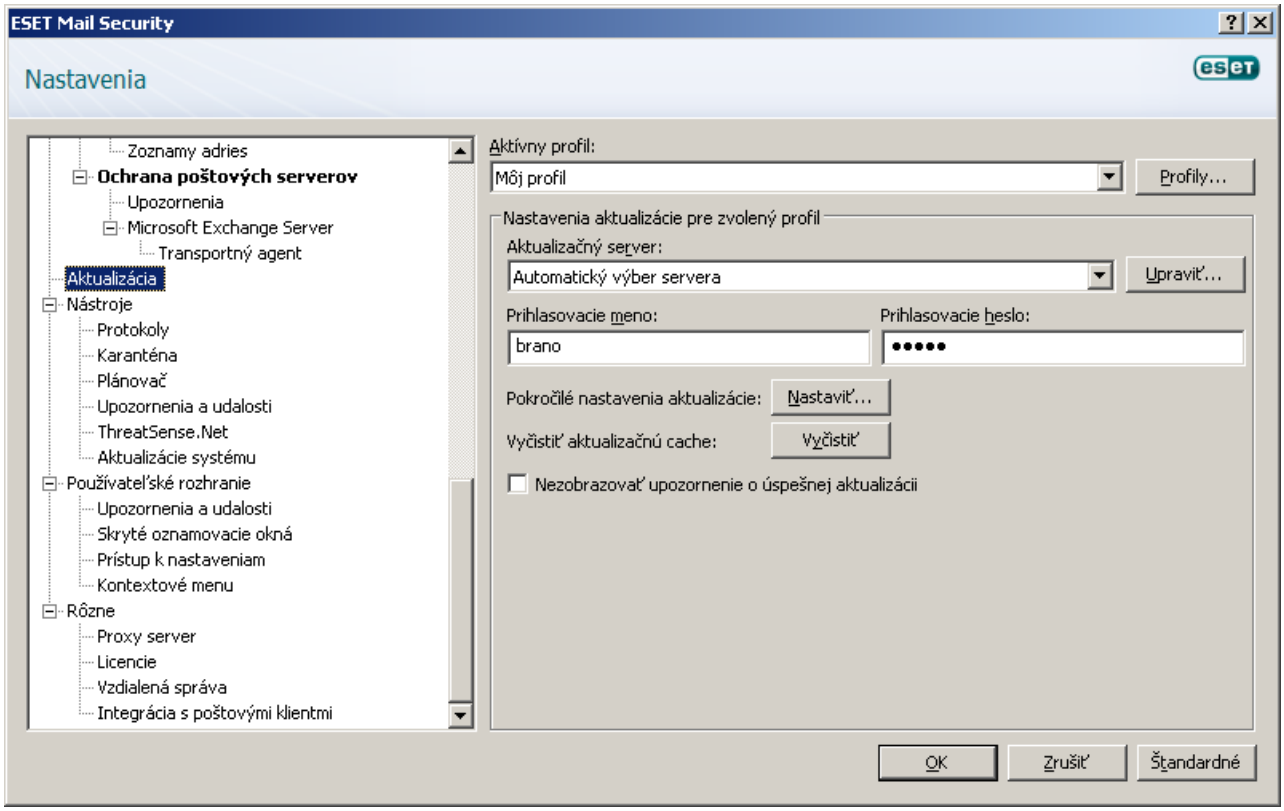
Poznámka: Odporúčame nastaviť rovnaký počet skenovacích jadier a vlákien kontroly.

3. Aktualizácia

Aktualizácia vírusových databáz a programových komponentov je dôležitá súčasť na zabezpečenie komplexnej ochrany pred škodlivým kódom. Jej nastaveniu a funkčnosti preto treba venovať zvýšenú pozornosť. Po kliknutí na voľbu **Aktualizácia** v hlavnom menu sa otvorí aktualizačné okno v pravej časti obrazovky. **Aktualizovať vírusovú databázu** spôsobí, že ESET Mail Securityskontroluje dostupnosť novšej databázy okamžite po stlačení. **Nastaviť meno a heslo...** umožňuje nastaviť meno a heslo dodané spoločnosťou ESET pre aktualizáciu produktu. Autorizačné údaje je možné nastaviť už počas inštalácie ESET Mail Security.

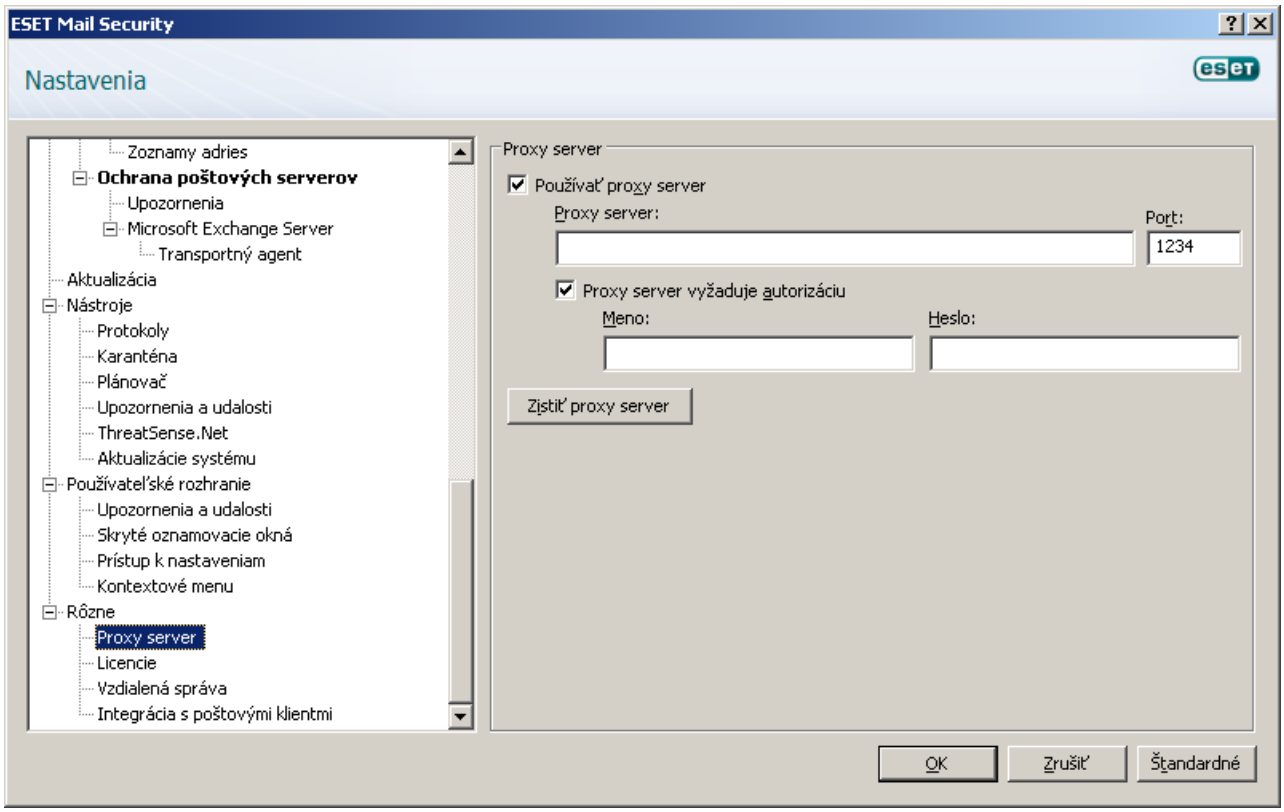


V pokročilých nastaveniach (dostupné po stlačení klávesy **F5**) sú ďalšie podrobné nastavenia aktualizácie (v strome pokročilých nastavení kliknite na vetvu **Aktualizácia**). Položku **Aktualizačný server** je vhodné nastaviť na **Automaticky vybrať server**. V tejto časti sa nachádza tlačidlo **Nastaviť**, ktoré umožňuje nastaviť podrobnejšie možnosti aktualizácie, ako nastavenie módu aktualizácie, prístupu cez proxy server, prístupu k aktualizácii v lokálnom mirrore a vytvárania kópie aktualizácie.



3.1 Nastavenie proxy servera

V prípadoch prístupu daného systému s ESET Mail Security na sieť cez proxy server je tento potrebné definovat v menu rozšírených nastavení (stlačte **F5** na klávesnici). V menu rozšírených nastavení kliknite na **Rôzne > Proxy server**. Označte možnosť **Používať proxy server** a v poliach vyplňte informácie o názve alebo ip adrese Vášho proxy servera (pole **Proxy server:**) a o porte ktorý používa (pole **Port:**). Ak je potrebné sa na proxy serveri, ktorý používa Vaše pripojenie autentifikovať, aktivujte pole **Proxy server vyžaduje autorizáciu** a vložte do polí **Meno:** a **Heslo:** potrebné autorizačné údaje.



V prípade neznalosti týchto informácií môže používateľ inicializovať pokus o zistenie nastavení proxy servera pre ESET Mail Security automaticky. Na tento účel slúži tlačidlo **Zistiť proxy server**.

Poznámka: Nastavenie Proxy servera môže byt iné pre konkrétny aktualizačný profil. V takom prípade sa toto nastavenie vykonáva v menu rozšírených nastavení (stlačte **F5** v hlavnom okne programu) vo vetve **Aktualizácia**.

4. ESET Mail Security - ochrana pre Microsoft Exchange Server

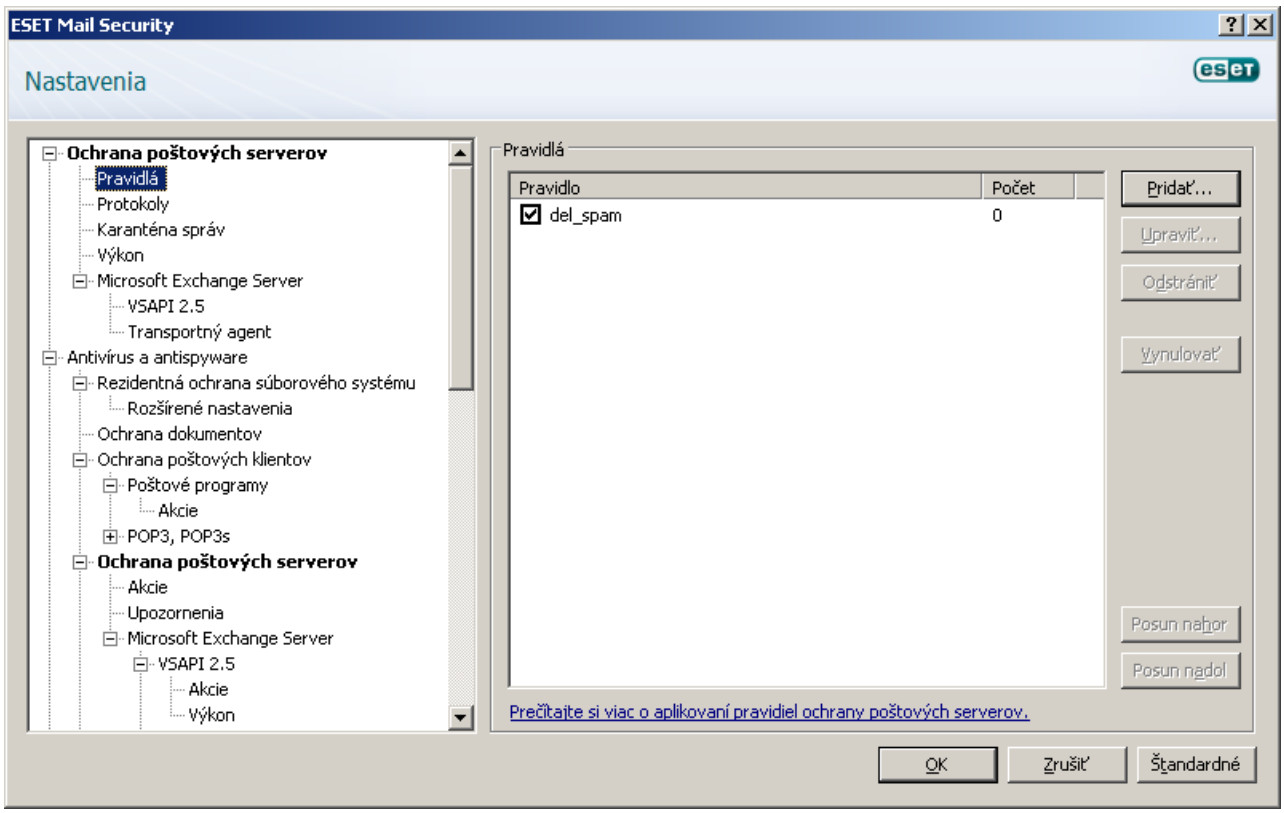
4.1 Všeobecné nastavenia

Táto časť bližšie opisuje ako spravovať pravidlá, súbory s protokolmi, karanténu správ a nastavenia výkonu.

4.1.1 Pravidlá

Pravidlá umožňujú administrátorom manuálne konfigurovať podmienky filtrovania správ a tiež vybrať akcie, ktoré sa s filtrovanými správami vykonajú. Pravidlá sa aplikujú na základe definovaných podmienok. Viaceré podmienky v rámci pravidla sú kombinované pomocou logického operátora AND, pričom pravidlo bude uplatnené len ak sú splnené všetky podmienky. Údaj v stĺpci **Počet** (vedľa každého názvu pravidla) zobrazuje počet úspešných použití pravidla.

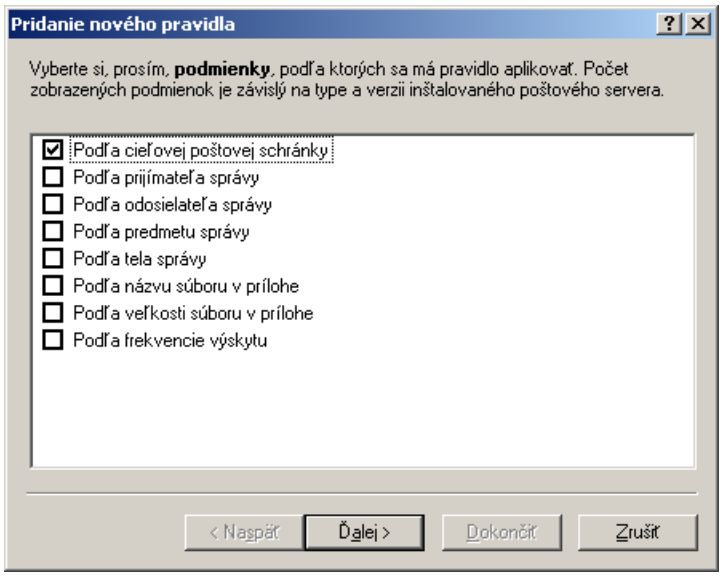
Pravidlá sa porovnávajú so správou pri jej spracovaní Transportným agentom (TA) alebo VSAPI. Ak je povolená kontrola správ prostredníctvom TA aj VSAPI, pri príchode správy sa počítadlo pravidiel môže zvýšiť aj o 2 alebo viac. VSAPI pristupuje k jednotlivým častiam správy (telo, príloha) osobitne a aj pravidlá sú aplikované na každú časť správy zvlášť. Ďalej sa pravidlá používajú aj počas kontroly na pozadí (napr. opakovaná kontrola poštovej schránky po aktualizácii vírusovej databázy), čo takisto prispieva k zvyšovaniu stavu počítadla.



Poznámka: Pri použití pravidiel sa dajú využiť aj systémové premenné (napríklad: *%PATHEXT%*).

4.1.1.1 Pridávanie nových pravidiel

Tento sprievodca Vás prevedie pridávaním Vašich vlastných pravidiel s kombinovanými podmienkami.



Poznámka: Nie všetky podmienky sú použiteľné ak je správa kontrolovaná transportným agetom.

- **Podľa cieľovej poštovej schránky** platí pre meno mailovej schránky (VSAPI)
- **Podľa prijímateľa správy** platí pre správu poslanú špecifickému prijímateľovi (VSAPI +TA)
- **Podľa odosieľateľa správy** platí pre správu poslanú od špecifického odosielateľa (VSAPI + TA)
- **Podľa predmetu správy** platí pre správy so špecifickým predmetom (VSAPI + TA)
- **Podľa tela správy** platí pre správy so špecifickým textom v tele správy (VSAPI)
- **Podľa názvu súboru v prílohe** platí pre správy so špecifickým názvom prílohy (VSAPI)
- **Podľa veľkosti súboru v prílohe** platí pre správy s veľkosťou prílohy presahujúcou definovanú veľkosť (VSAPI)
- **Podľa frekvencie výskytu** platí pre objekty (správy alebo prílohy) ktorých výskyt za nastavený čas presahuje špeficikovaný počet. Toto je obzvlášť užitočné ak Vám neustále prichádzajú spamové správy s tým istým telom správy alebo tou istou prílohou (VSAPI + TA)

Pri nastavovaní horeuvedených podmienok (okrem **Podľa veľkosti súboru v prílohe**) stačí uviesť iba časť frázy, ak nie je zapnutá možnosť **Porovnávať ako celé slová**. Ak nie je zapnutá možnosť **Rozlišovať veľkosť písmen**, tak veľkosť písmen sa neberie do úvahy. Ak používate iné hodnoty ako alfanumerické znaky, použite zátvorky a úvodzovky. Pri tvorení podmienok môžete použiť aj logické operátory AND, OR a NOT ("A", "ALEBO" a "NIE").

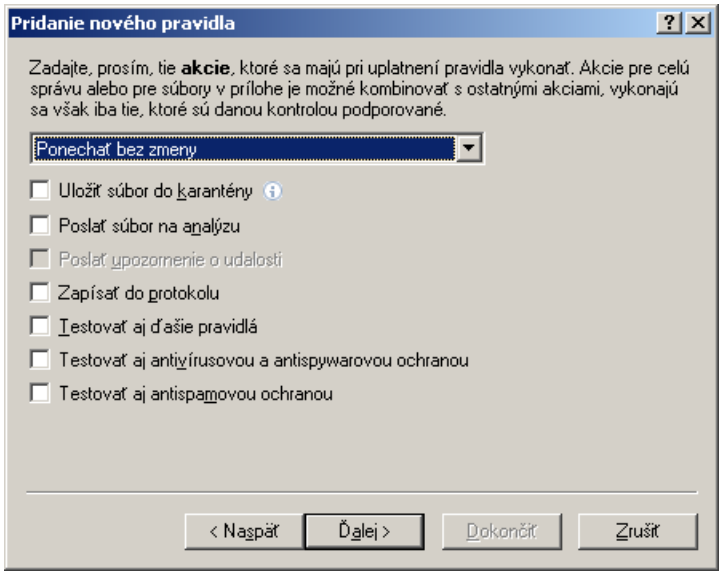
Poznámka: Microsoft Exchange Server 2000 (VSAPI 2.0) vyhodnocuje iba zobrazované meno prijímateľa/ odosielateľa, nie e-mailovú adresu. Vyhodnocovanie e-mailových adries je podporované od verzie Microsoft Exchange Server 2003 (VSAPI 2.5) a vyššie.

Príklady zadávania podmienok:

Podľa cieľovej poštovej schránky	smith
Podľa odosielateľa správy	smith@mail.com
Podľa prijímateľa správy	“J.Smith” or “smith@mail.com”
Podľa predmetu správy:	“ ”
Podľa názvu súboru v prílohe:	“.com” OR “.exe”
Podľa tela správy:	(“free” OR “lottery”) AND (“win” OR “buy”)

4.1.1.2 Akcie

V tejto sekcii môžete vyberat aké akcie budú vykonané so správami a/alebo prílohami, ktoré spadajú pod podmienky definované v pravidlách. Nemusíte vykonat žiadnu akciu, môžete oznacit správu ako hrozbu/spam alebo správu úplne vymazat. V prípade, že správa spadá do podmienok ktoréhokolvek pravidla, nebude už kontrolovaná antivírusom alebo antispamom, ak nie je táto funkcionalita explicitne aktivovaná oznacením príslušného zaškrtávaciaho pola v spodnej casti okna (v takom prípade vykonané akcie závisia od antivírusových/antispamových nastavení).



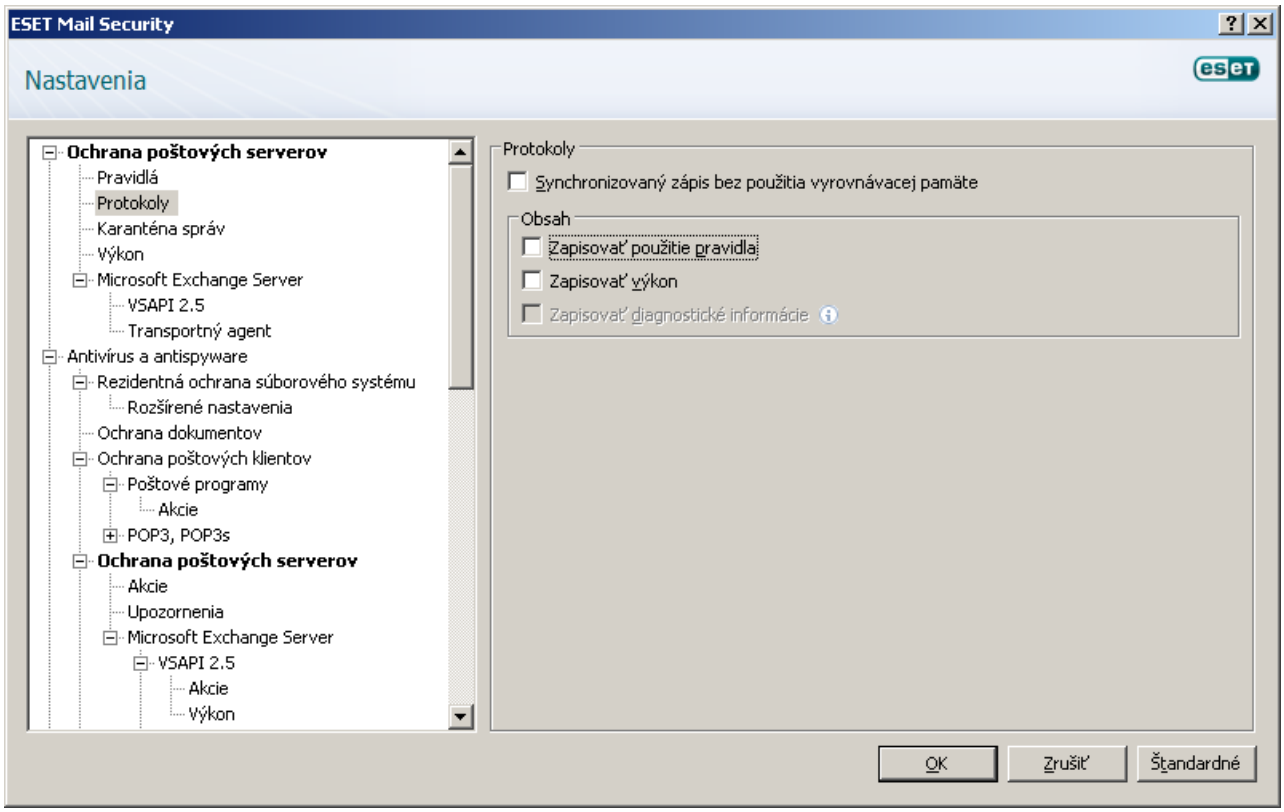
- **Ponechat bez zmeny** - so správou nebude vykonaná žiadna akcia
- **Oznacit ako neliecenú infiltráciu** - oznací správu ako keby obsahovala nevyliecenú infiltráciu (nezávisle od toho ci ju naozaj obsahuje)
- **Oznacit ako nevyžiadanú poštu** - oznací správu ako spam (bez ohladu na to ci je alebo nie je spam). Táto možnost nie je dostupná, ak používate ESET Mail Security bez Antispam modulu.
- **Zmazat správu** - odstráni celú správu aj s obsahom, ak sú splnené podmienky

- **Uložit súbor do karantény** uloží priložený súbor do karantény
  Poznámka: Nepomýlte si túto karanténu s karanténou e-mailových správ (vid. kapitola Karanténa e-mailových správ 24).
- **Poslat súbor na analýzu** odošle podozrivé prílohy na analýzu do vírusového laboratória ESET
- **Poslat upozornenie o udalosti** pošle oznam administrátorovi (v závislosti od nastavení v **Nastavenia > Upozornenia**).
- **Zapísat do protokolu** zapíše informáciu o použitom pravidle do protokolu
- **Testovat aj dašie pravidlá** povolí vyhodnocovanie dalších pravidiel, cím umožní používatelovi nastavit viac sústav podmienok a naväzujúcich akcií.
- **Testovat aj antivírusovou a antispywarovou ochranou** preskenuje správu aj jej prílohu
- **Testovat aj anstispamovou ochranou** preskenuje správu antispamovým modulom

Posledný krok vo vytváraní nového pravidla je pomenovanie každého z vytvorených pravidiel. Môžete pridat aj komentár k pravidlu. Táto informácia sa uloží do protokolu Microsoft Exchange Servera.

4.1.2 Súbory s protokolmi

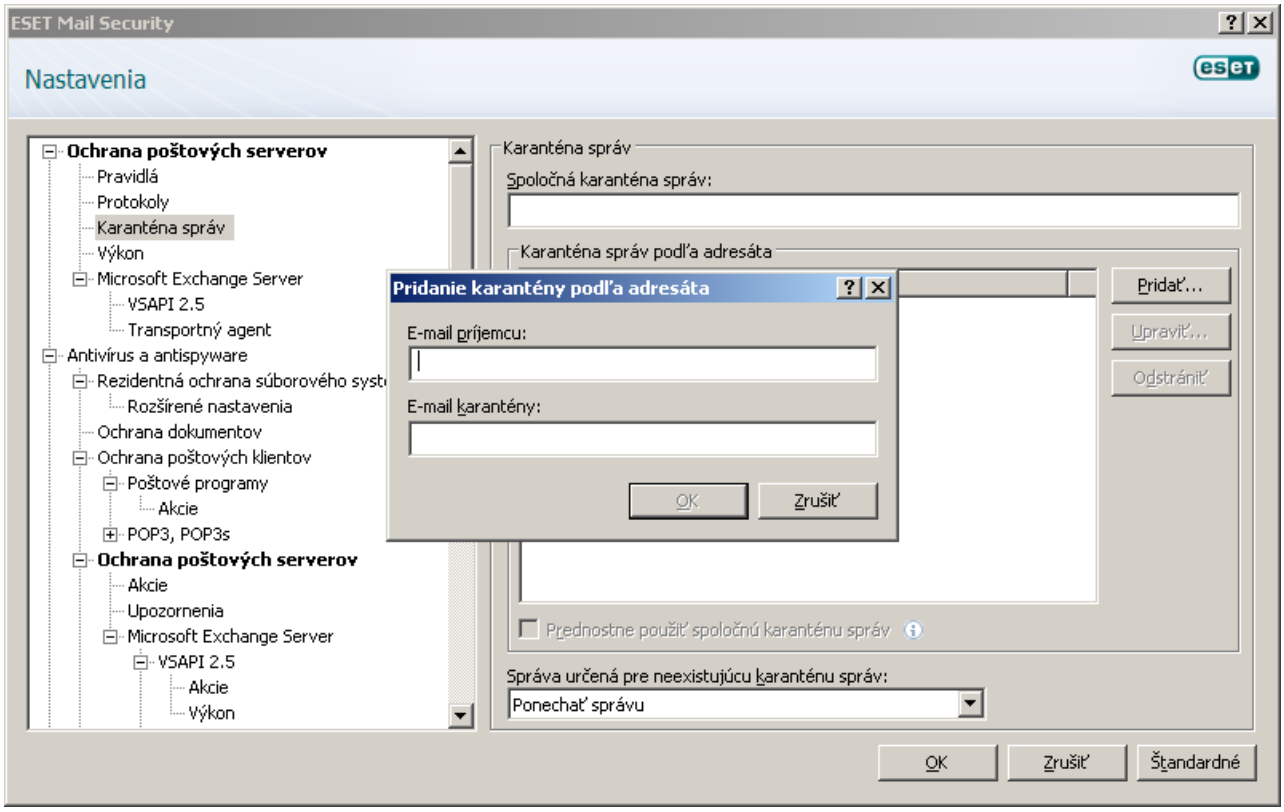
V nastaveniach protokolov si môžete upraviť obsah, ktorý sa do súboru s protokolom bude zapisovať. Detailnejší protokol obsahuje viac informácií, ale môže mať negatívny dopad na výkon servera.



Ak je zapnutý **Synchronizovaný zápis bez použitia vyrovnávacej pamäte** všetky záznamy protokolu sa hneď zapíšu do súboru, bez toho aby boli najprv uložené vo vyrovnávacej pamäti. Štandardne si komponenty ESET Mail Security, ktoré bežia pod systémom Microsoft Exchange Server, ukladajú správy určené do protokolov do svojej internej pamäte a posielajú ich aplikačnému protokolu v pravidelných časových intervaloch tak, aby neznižovali výkon servera. Tu môže nastať situácia, kedy sa nemusí zachovať chronologická integrita diagnostických záznamov v protokole. Odporúčame toto nastavenie nezapínať, kým to nie je potrebné pre účely diagnostiky. V časti **Obsah** môžete nastaviť typy informácií, ktoré sa budú do protokolov zapisovať.

4.1.3 Karanténa správ

Poštový adresár **Karanténa správ** je špeciálny adresár nastavený systémovým administrátorom, ktorý slúži ako úložisko potenciálne infikovaných správ a spamu. Správy uložené v karanténe sa dajú analyzovať, prípadne aj liečiť pomocou novšej vírusovej databázy.



Adresu karantény správ môžete nastaviť v poli **Spoločná karanténa správ** (napr. hlavna_karantena@spoločnosť.sk). Takisto je možné využiť interný systém karantény systému Microsoft Exchange Server 2007/2010 a to tak, že toto pole necháte prázdne a z roletového menu (v spodnej časti) vyberiete **Uložiť do systémovej karantény správ poštového servera** (ak bola nadefinovaná administrátorom). Správy sa potom doručia do karantény interným mechanizmom systému Microsoft Exchange Server na základe jeho vlastných nastavení.

V poli **Karanténa správ podľa adresáta** môžete nastaviť viacero karanténnych adries pre viacero príjemcov. Pravidlá karantén možno vypínať a zapínať podľa potreby označovaním/odznačovaním príslušných zaškrtávacích polí.

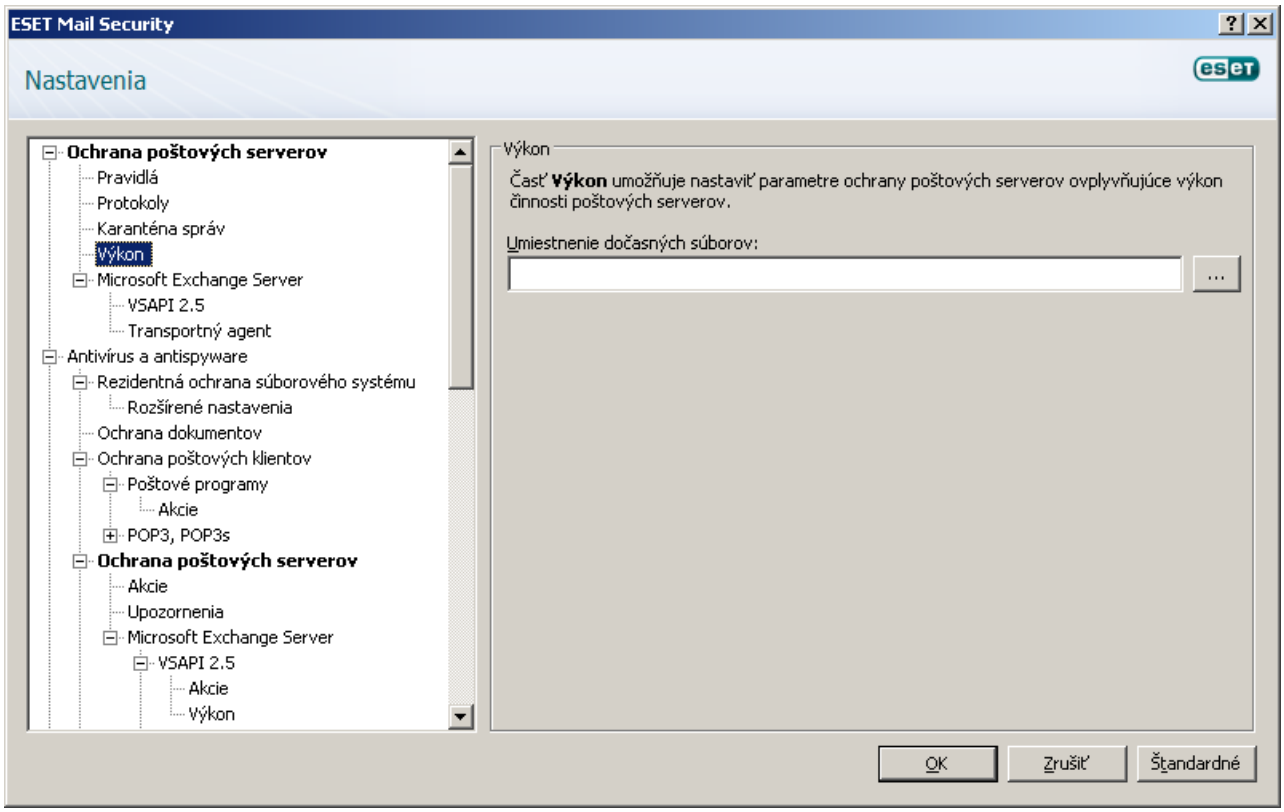
Poznámka: Pri nastavovaní správy karantén môžete použiť aj sytémové premenné (napríklad: *%PATH%*).

4.1.3.1 Pridanie nového pravidla karantény

Zadajte požadovanú e-mailovú adresu príjemcu a e-mailovú adresu karantény do príslušných polí.
Ak chcete vymazať e-mailovú správu určenú pre prijímateľa, ktorý nemá pridelené karanténne pravidlo, označte v roletovom menu **Správa určená pre neexistujúcu karanténu správ: možnosť Ponechať správu**.

4.1.4 Výkon

V tejto časti môžete určiť adresár, v ktorom sa budú ukladať dočasné súbory, čo umožňuje zvýšiť výkon programu. Ak nebol určený žiaden adresár, ESET Mail Security bude vytvárať dočasné súbory v dočasnom systémovom adresári.

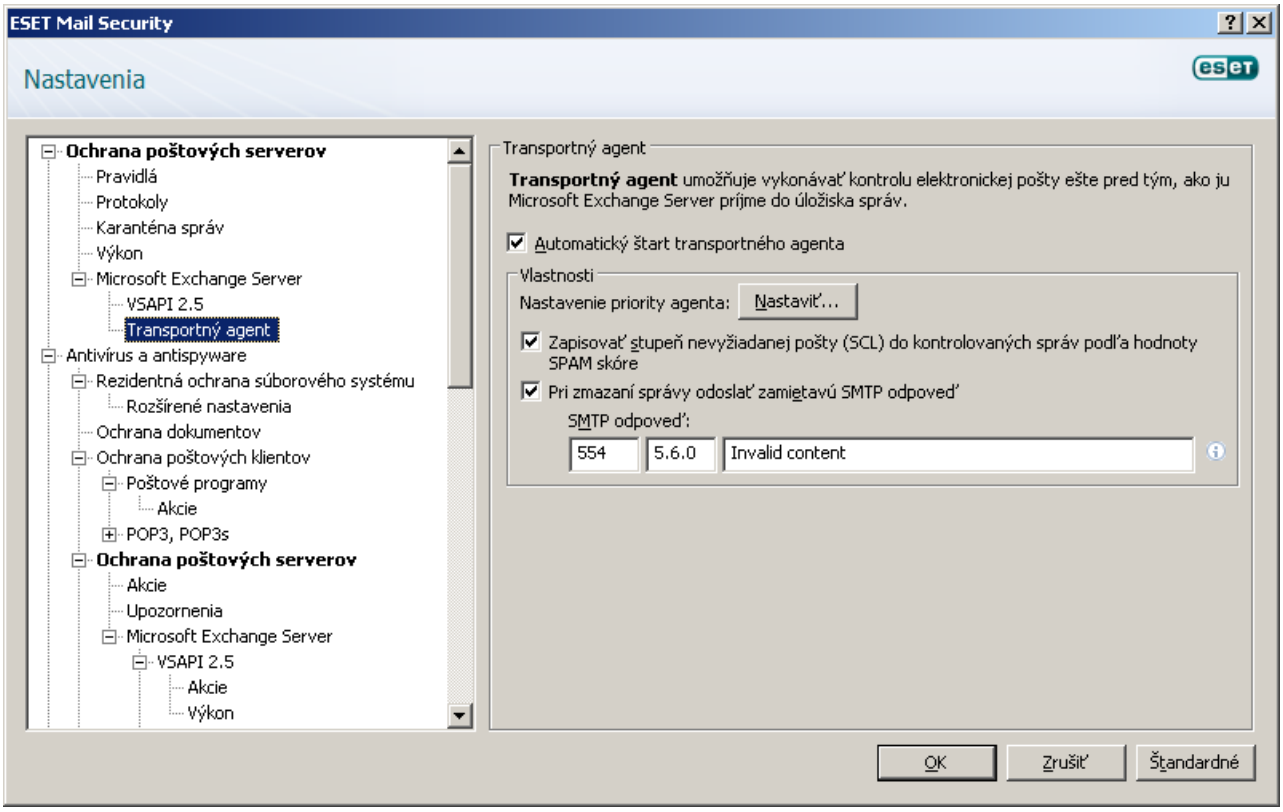


Poznámka: Pre účely minimalizácie negatívneho vplyvu zo fragmentácie a zdržania pri čítaní a zápise Vám odporúčame dočasný adresár umiestniť na inom harddisku ako je Vaša inštalácia Microsoft Exchange Server. Odporúčame vyhnúť sa ukladaniu dočasného adresára na vymeniteľné médiá ako diskety, USB kľúče, DVD atď.

Poznámka: Aj tu je možné používať systémové premenné (napr. *%SystemRoot%*\TEMP).

4.1.5 Transportný agent

V tejto časti môžete nastaviť automatické spúšťanie (a prioritu spúšťania) transportného agenta. Na systémoch Microsoft Exchange Server 2007 a novších sa dá transportný agent nainštalovať iba ak je server v jednej z týchto dvoch rolí: *Edge Transport* alebo *Hub Transport*.



Poznámka: Transportný agent nie je vo verzii Microsoft Exchange Server 5.5. (VSAPI 1.0).

V menu **Nastavenie priority agenta** môžete nastavovať priority agentov ESET Mail Security. Číselný rozsah priority agenta závisí od verzie Microsoft Exchange Server (čím je číslo nižšie, tým väčšia je priorita).

Zapisovať stupeň nevyžiadanej pošty (SCL) do záhlavia kontrolovaných správ podľa hodnoty SPAM skóre - SCL je hodnota pridelená správe, ktorá indikuje pravdepodobnosť, že správa je spam (vyhodnocujú sa špecifiká hlavičky správy, predmetu, obsahu, atď.). Hodnotenie 0 znamená, že je veľmi nepravdepobné aby bola konkrétna správa spam, kým hodnotenie 9 zasa poukazuje na vysokú pravdepodobnosť spamu. Hodnoty SCL možno ďalej spracovávať technológiou Intelligent Message Filter (alebo Content Filter Agent) systému Microsoft Exchange Server. Podrobnejšie informácie nájdete v dokumentácii k Microsoft Exchange Server.

Možnosť **Pri zmazaní správy odoslať zamietavú SMTP odpoveď**:

- Ak je táto voľba vypnutá, server pošle OK SMTP odpoveď v znení '250 2.5.0 – Requested mail action okay, completed' odosielateľovmu MTA (Mail Transfer Agent) a potom vykoná tzv. silent drop.

- Ak je voľba zapnutá, odosielateľovmu MTA sa pošle SMTP reject odpoveď (SMTP zamietnuté). Odpoveď môžete napísať v takomto formáte:

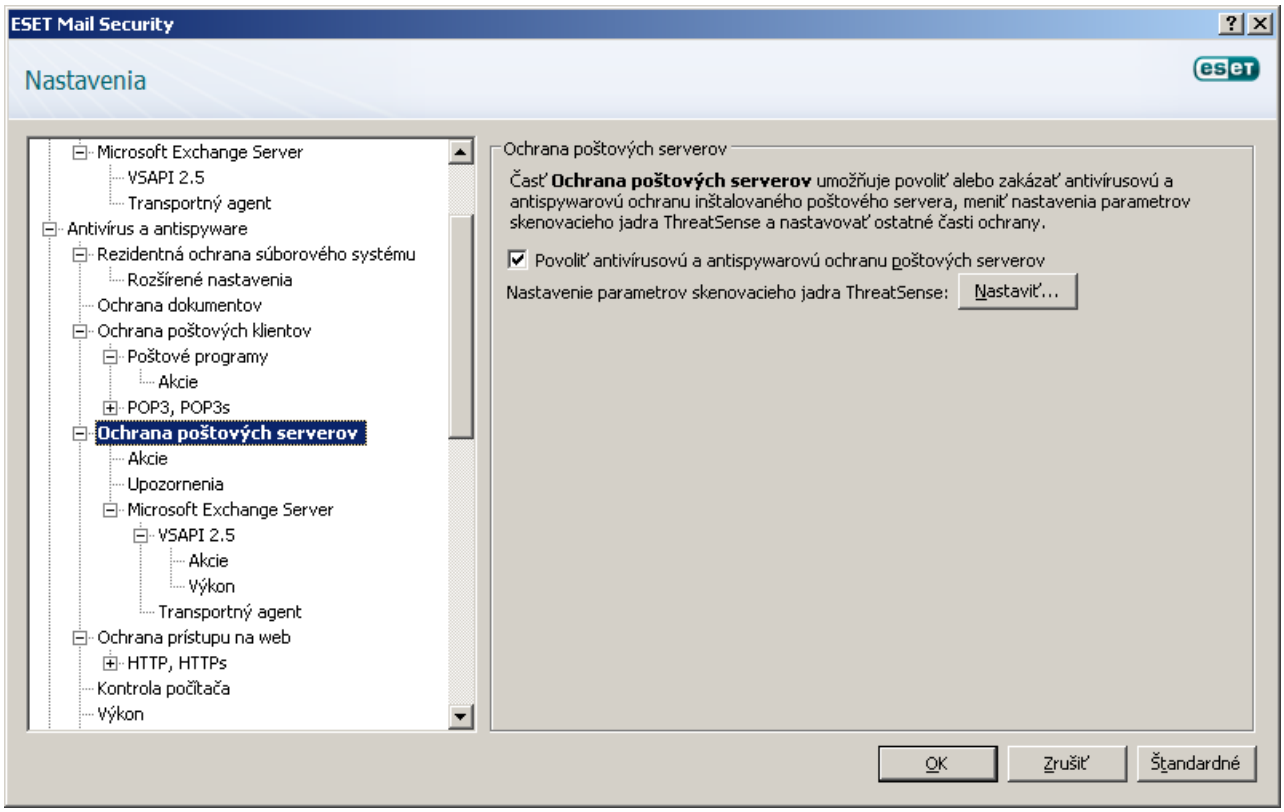
Primárny kód odpovede	Doplnkový kód stavu	Popis
250	2.5.0	Requested mail action okay, completed
451	4.5.1	Requested action aborted: local error in processing
550	5.5.0	Requested action not taken: mailbox unavailable

Pozor!: Použitie nesprávnej syntaxe v kódoch odpovedí, môže viesť k znefunčkneniu programových komponentov a zníženiu efektivity.

Poznámka: Pri nastavovaní SMTP Reject odpovedí môžete použiť aj systémové premenné.

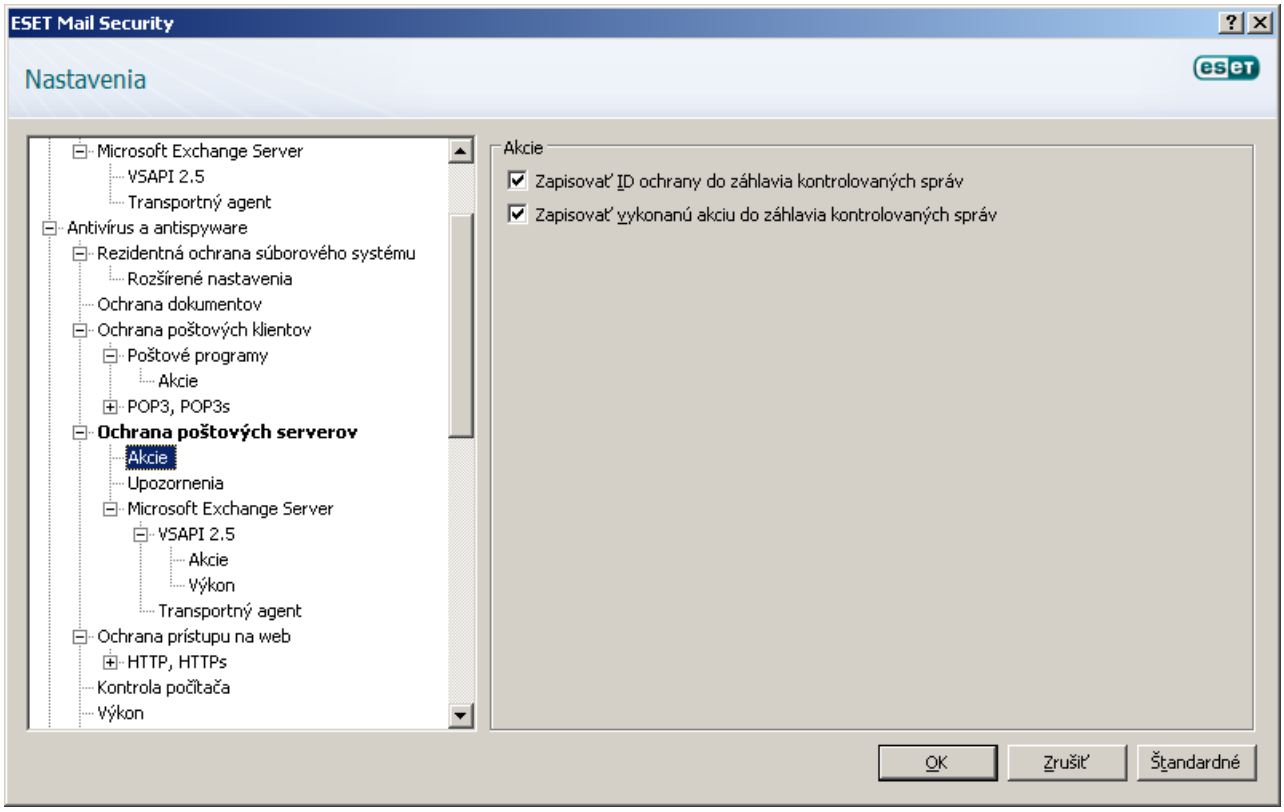
4.2 Nastavenia antivirus a antispyware

Označením možnosti **Povoliť antivírusovú a antispywarovú ochranu poštových serverov** zapnete antivírusovú a antispyware ochranu poštového servera.Táto sa zapne vždy automaticky po každom reštarte servera.



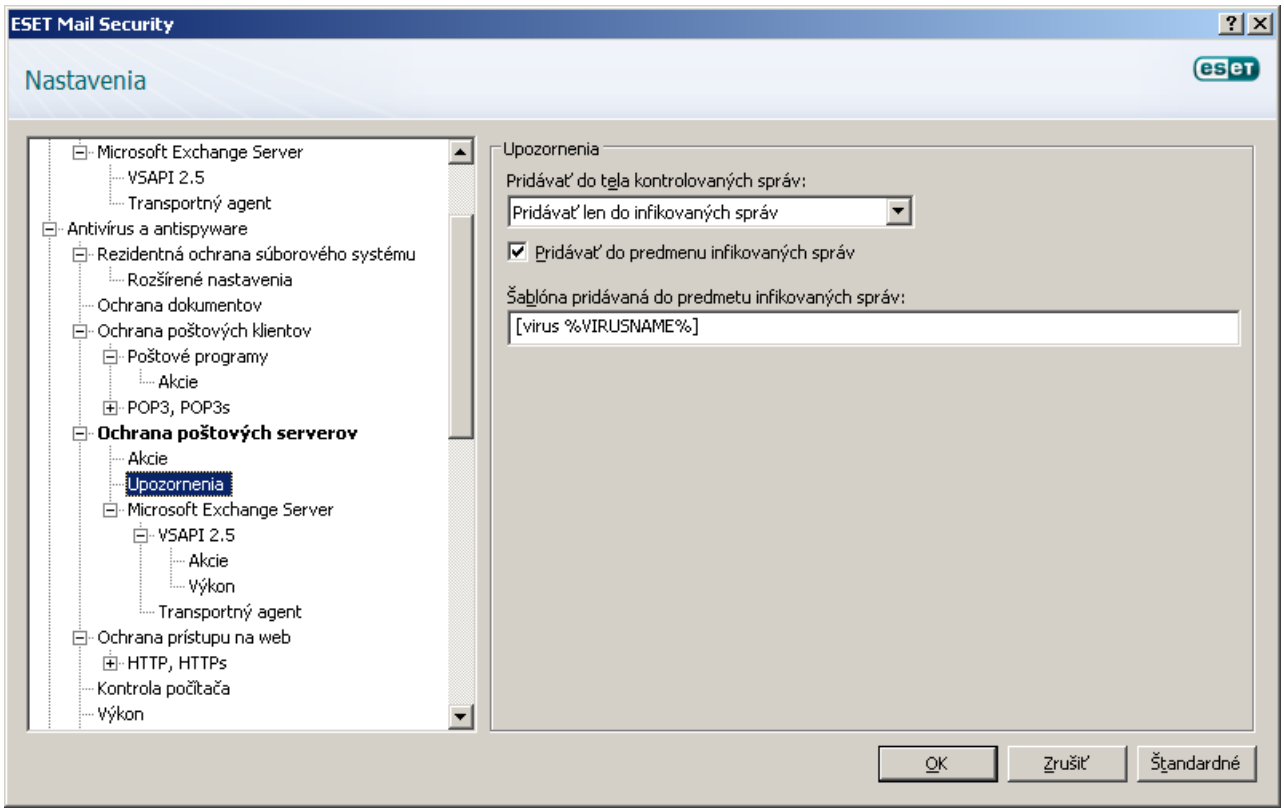
4.2.1 Akcie

V tejto sekcii môžete zapnúť pridávanie ID kódu skenovacej úlohy a tiež vykonanej akcie do hlavičky kontrolovaných správ.



4.2.2 Upozornenia

ESET Mail Security Vám ponúka možnosť pridávať text k pôvodnému predmetu, alebo priamo do tela infikovaných správ.

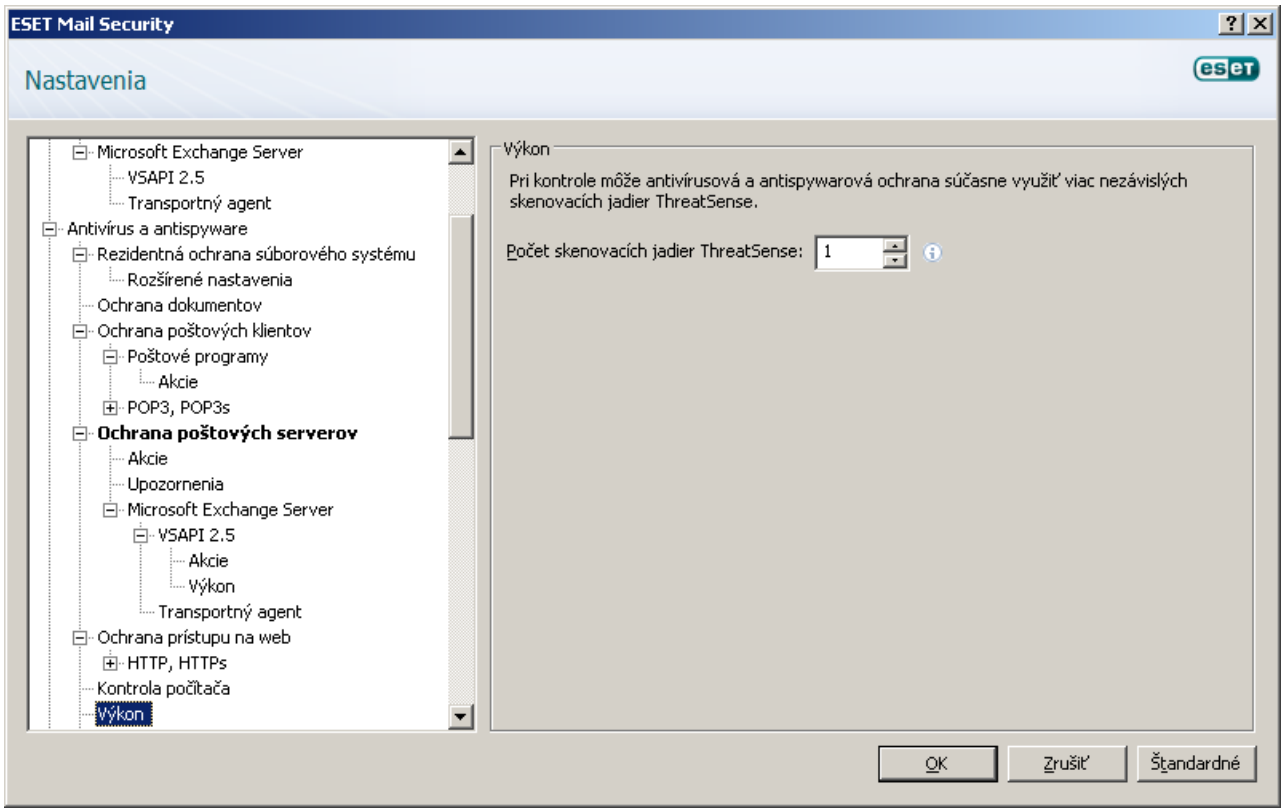


Ak zapnete možnosť **Pridávať do predmetu infikovaných správ**, ESET Mail Security pridá do predmetu e-mailovej správy text zadefinovaný v textovom poli **Šablóna pridávaná do predmetu infikovaných správ:** (prednastavené je [virus %VIRUSNAME%]). Horeuvedené nastavenia môžu automatizovať filtrovanie infikovaných správ triedením správ do vlastných adresárov podľa slov v predmete správy (ak túto funcionalitu podporuje váš poštový klient).

Poznámka: Pri zostavovaní textu, ktorý sa pridá do predmetu správy môžete použiť aj systémové premenné.

4.2.3 Výkon

V tejto sekcii môžete nastaviť počet skenovacích jadier ThreatSense, ktoré budú použité pri antivírusovej kontrole. Použitie viacerých skenovacích jadier ThreatSense na systémoch s viacerými procesormi môže zvýšiť rýchlosť kontroly.

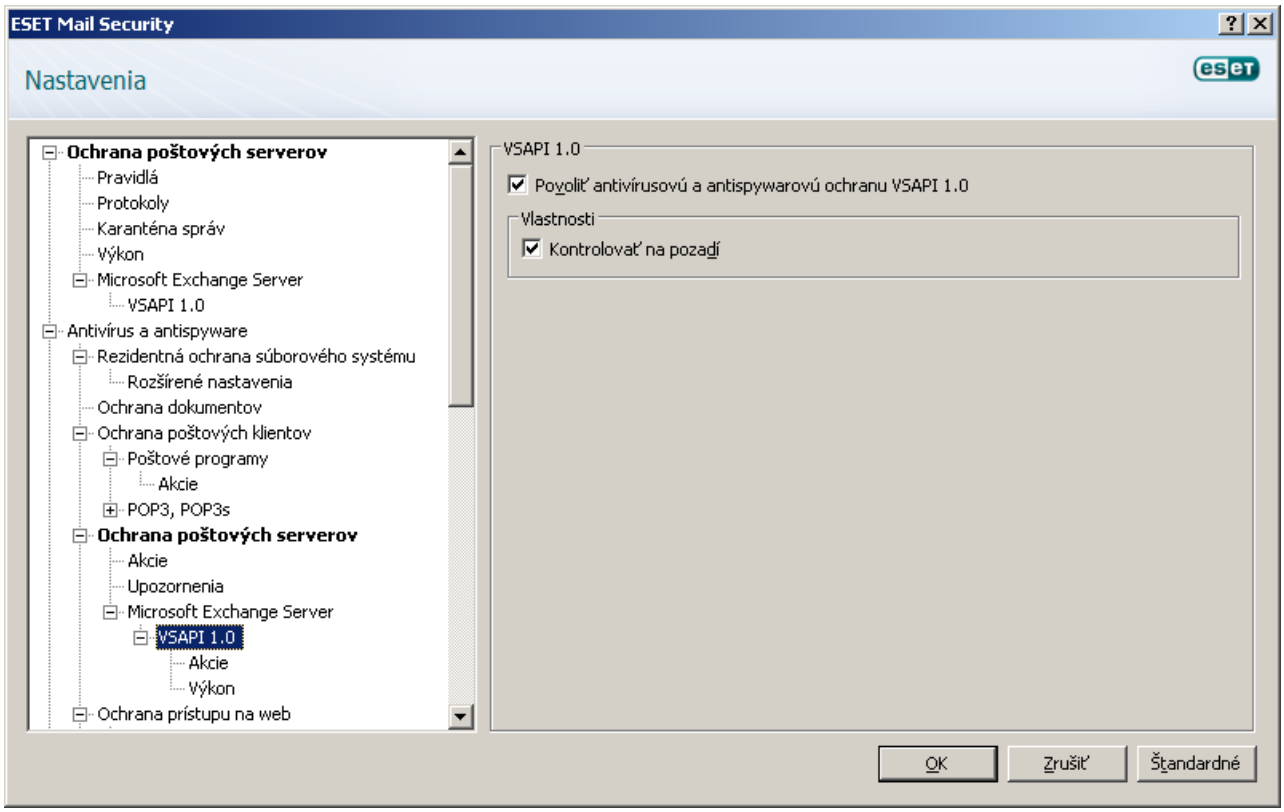


4.2.4 Virus-Scanning Application Programming Interface (VSAPI)

Microsoft Exchange Server je vybavený mechanizmom, ktorý zabezpečuje, že každá časť správy sa prekontroluje najnovšou vírusovou databázou. Ak správa alebo jej časť ešte nebola skontrolovaná, táto bude oskenovaná skôr ako sa uvoľní pre klienta. Každá podporovaná verzia Microsoft Exchange Server (5.5/2000/2003/2007/2010) ponúka odlišnú verziu VSAPI.

4.2.4.1 Microsoft Exchange Server 5.5 (VSAPI 1.0)

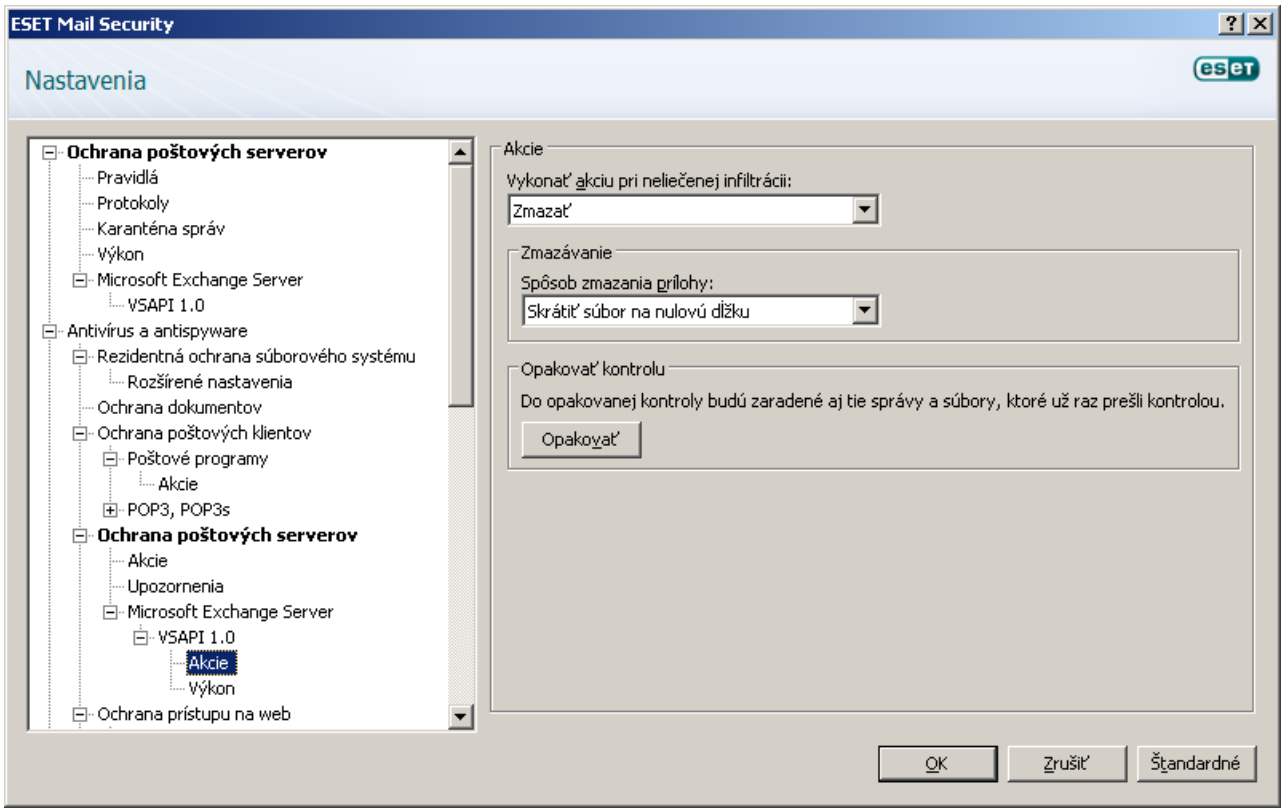
Táto verzia Microsoft Exchange Server obsahuje VSAPI verziu 1.0.



Možnosť **Kontrolovať na pozadí** umožní kontrolu všetkých správ na pozadí systému. Microsoft Exchange Server si sám určuje, či prebehne kontrola správ okamžite alebo neskôr, a to na základe rôznych faktorov ako sú napríklad momentálne zaťaženie servera, počet aktívnych používateľov, atď. Microsoft Exchange Server si uchováva záznam o kontrolovaných správach a verzii vírusovej databázy použitej pri skenovaní. Ak sa používateľ pokúša otvoriť správu, ktorá nebola skontrolovaná najnovšou verziou vírusových databáz, Microsoft Exchange Server pošle správu najprv na kontrolu ESET Mail Security a až potom ju umožní otvoriť vo Vašom poštovom klientovi.
Keďže kontrola na pozadí môže zvýšiť nároky na systém (kontrola prebieha po každej aktualizácii vírusovej databázy), odporúčame Vám používať plánovanú kontrolu mimo pracovného času. Plánovanú kontrolu na pozadí môžete nastaviť pridaním úlohy v Plánovači. Ak zadefinujete úlohu na vykonanie kontroly na pozadí môžete určiť čas spustenia, počet opakovaní a množstvo iných parametrov dostupných v Plánovači. Po naplánovaní úlohy sa táto zobrazí v zozname naplánovaných úloh, v ktorom ju tiež môžete upravovať, vymazať, alebo ju dočasne deaktivovať.

4.2.4.1.1 Akcie

V tejto časti môžete nastaviť akcie, ktoré sa vykonajú v prípade, že správa a/alebo príloha bola vyhodnotená ako infikovaná.



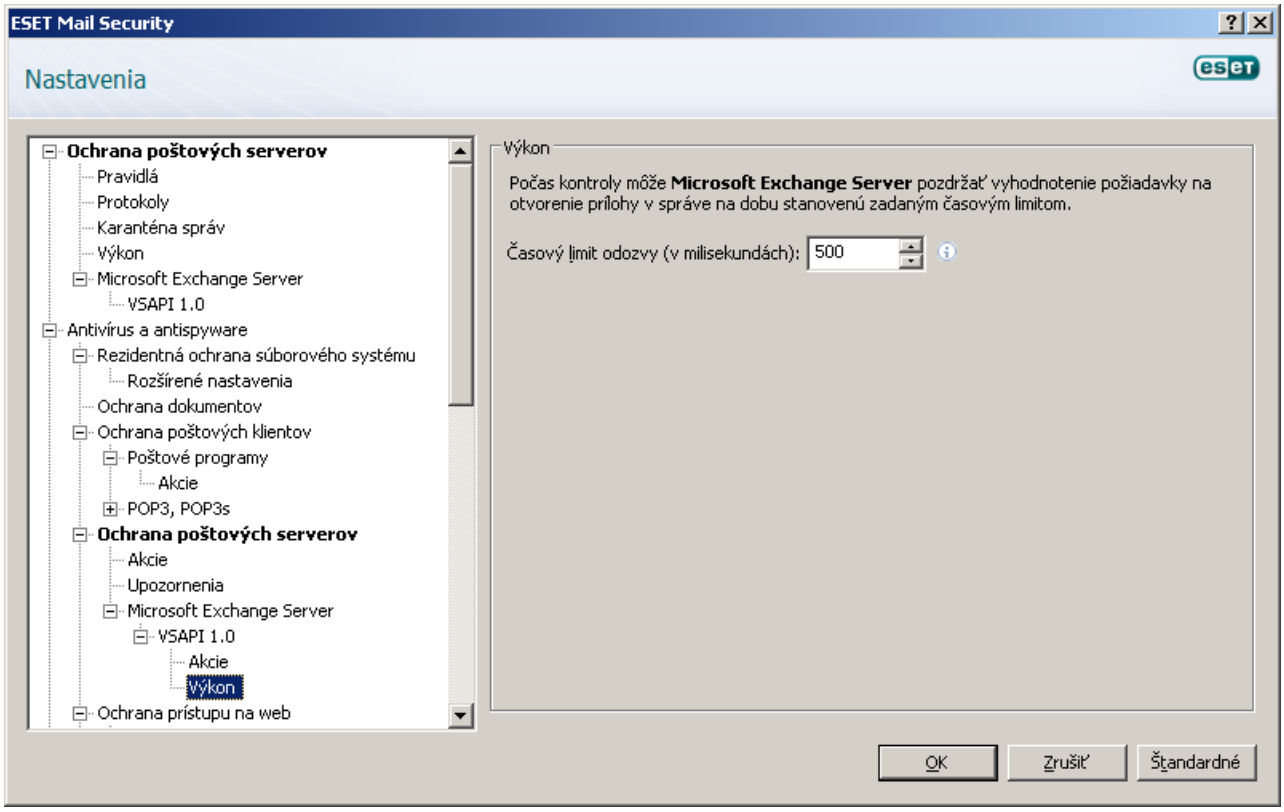
Pole **Vykonať akciu pri neliečenej infiltrácii** určí, či sa škodlivý obsah zablokuje alebo sa vymaže celá správa. Táto akcia bude použitá len ak sa pri automatickom liečení (ako je definované v **Nastavenie parametrov skenovacieho jadra ThreatSense > Liečenie**) nepodarilo správu vyliečiť.

Možnosť **Zmazávanie** umožnuje zredukovať veľkosť prílohy na nulovú hodnotu alebo nahradiť infikovaný súbor vírusovým protokolom alebo názvom pravidla.

Kliknutím na **Opakovať kontrolu** program znovu prekontroluje aj správy, ktoré už boli testované.

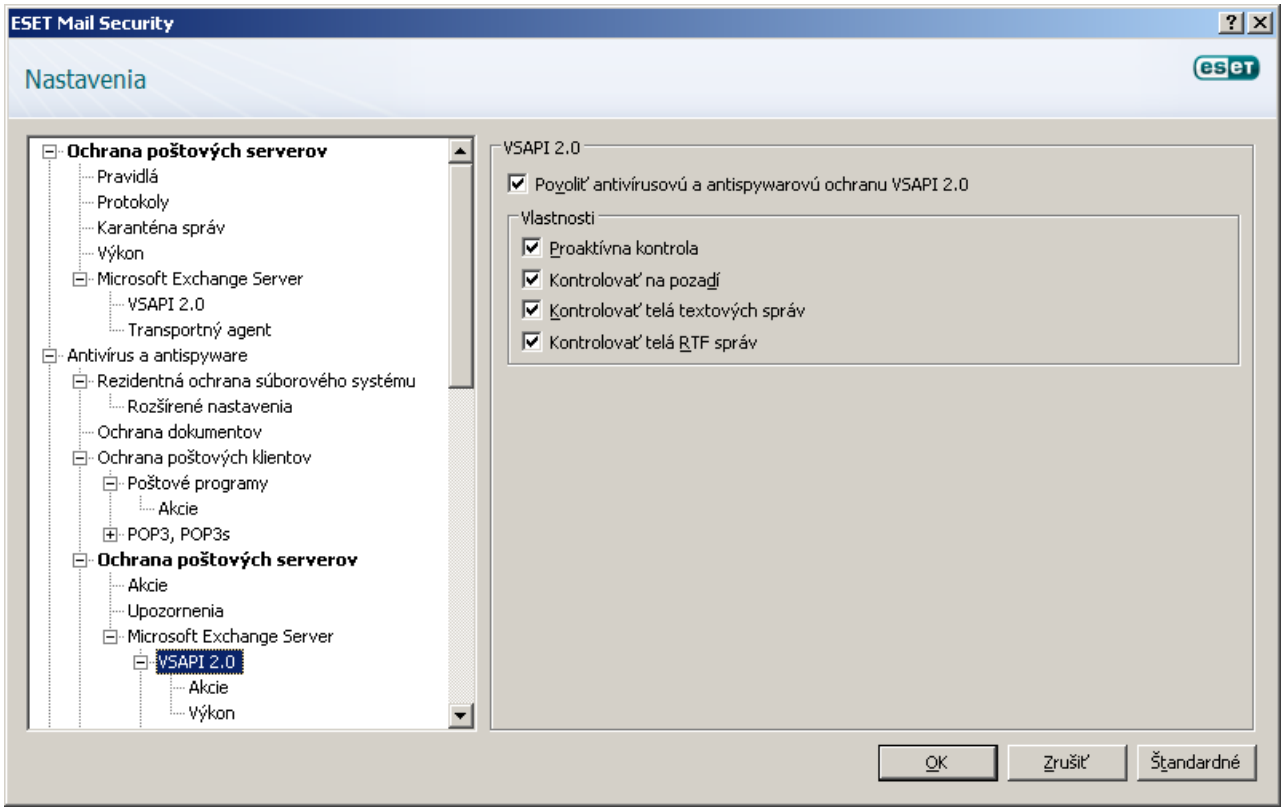
4.2.4.1.2 Výkon

Microsoft Exchange Server umožňuje počas kontroly obmedziť čas na otváranie príloh správ. Tento čas sa nastavuje v poli **Časový limit odozvy (v milisekundách):** a predstavuje dobu po ktorej sa klient znovu pokúsi pristúpiť k súboru, ktorý predtým nebol dostupný.



4.2.4.2 Microsoft Exchange Server 2000 (VSAPI 2.0)

Táto verzia Microsoft Exchange Server obsahuje VSAPI verziu 2.0



Ak je zapnutá možnosť **Proaktívna kontrola** nové prichádzajúce správy budú kontrolované v tom istom poradí ako boli prijaté.

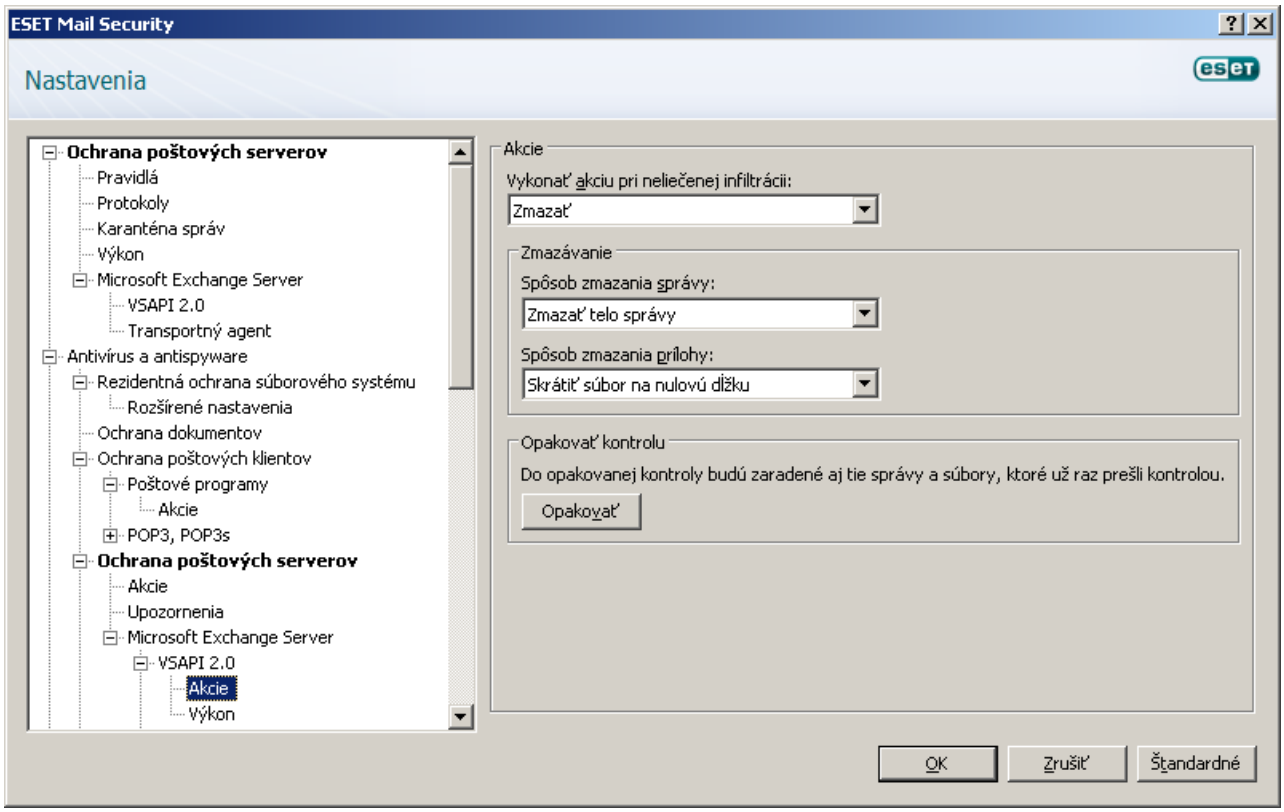
Možnosť **Kontrolovať na pozadí** umožní kontrolu všetkých správ na pozadí systému. Microsoft Exchange Server si sám určuje, či prebehne kontrola správ okamžite alebo neskôr, a to na základe rôznych faktorov ako sú napríklad momentálne zaťaženie servera, počet aktívnych používateľov, atď. Microsoft Exchange Server si uchováva záznam o kontrolovaných správach a verzii vírusovej databázy použitej pri skenovaní. Ak sa používateľ pokúša otvoriť správu, ktorá nebola skontrolovaná najnovšou vírusovou databázou, Microsoft Exchange Server pošle správu najprv na kontrolu ESET Mail Security kým ju umožní otvoriť vo Vašom poštovom klientovi.
Kedže kontrola na pozadí systému môže zvýšiť nároky na systém (kontrola prebieha po každej aktualizácii vírusovej databázy), odporúčame Vám používať plánovanú kontrolu mimo pracovného času. Plánovanú kontrolu na pozadí môžete nastaviť pridaním úlohy v Plánovači. Ak zadefinujete úlohu na vykonanie kontroly na pozadí, môžete určiť čas spustenia, počet opakovaní a množstvo iných parametrov dostupných v Plánovači. Po naplánovaní úlohy sa táto zobrazí v zozname naplánovaných úloh, v ktorom ju tiež môžete upravovať, vymazať, alebo ju dočasne deaktivovať.

Ak chcete aby boli kontrolované správy s obyčajným textom označte možnosť **Kontrolovať telá textových správ**.

Ak povolíte možnosť **Kontrolovať telá RTF správ** zapne sa kontrola tiel RTF správ.

4.2.4.2.1 Akcie

V tejto časti môžete nastaviť akcie na vykonanie v prípade, že správa a/alebo príloha bola vyhodnotená ako infikovaná.



Pole **Vykonať akciu pri neliečenej infiltrácii** určí, či sa škodlivý obsah zablokuje alebo sa vymaže celá správa. Táto akcia bude použitá len ak sa pri automatickom liečení (ako je definované v **Nastavenie parametrov skenovacieho jadra ThreatSense > Liečenie**) nepodarilo správu vyliečiť.

Možnosť **Spôsob zmazania tela správy** ponúka alternatívu, ktorá spočíva v zmazaní tela správy, alebo ďalšiu, ktorá prepíše telo správy informáciou o vykonanej akcii.

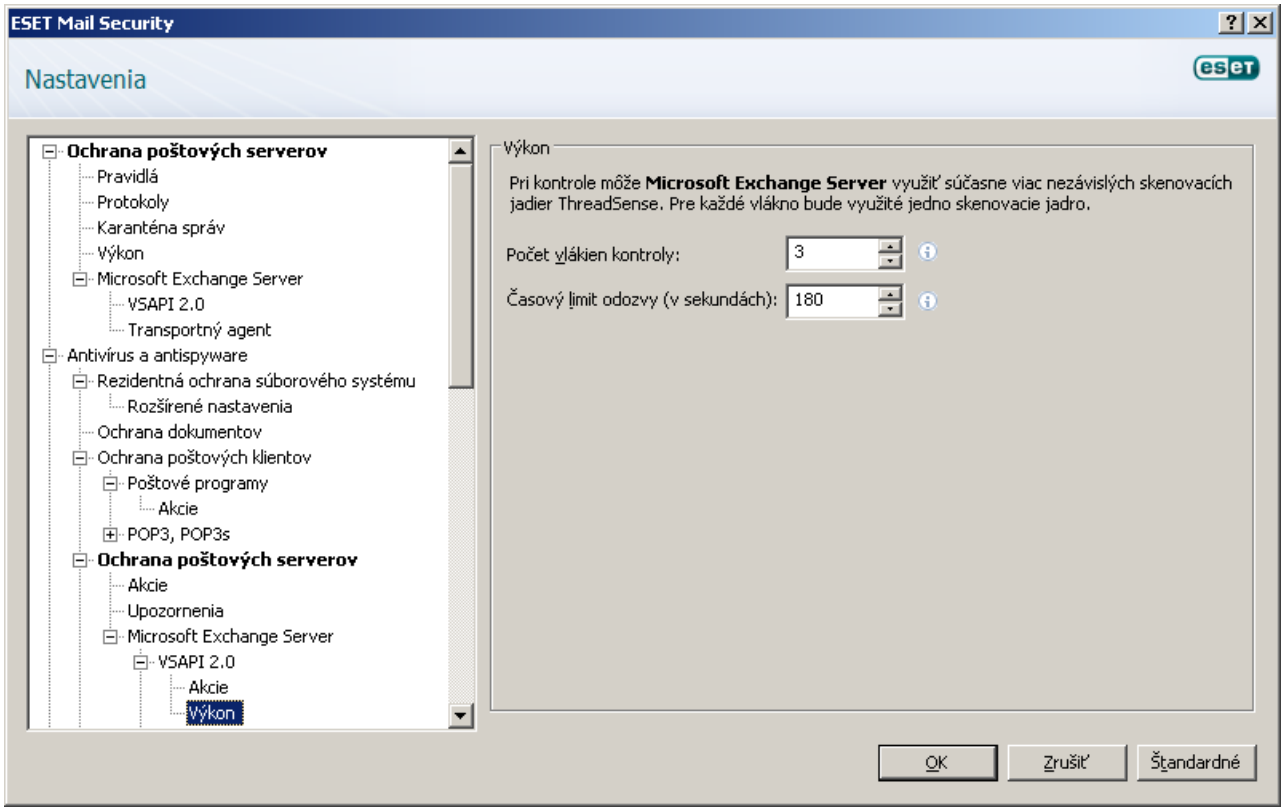
Spôsob zmazania prílohy určuje, či sa vymaže celá správa, alebo sa redukuje veľkosť prílohy na nulu, alebo sa infikovaný súbor nahradí informáciou o vykonanej akcii.

Kliknutím na **Opakovať kontrolu** program znovu prekontroluje aj správy, ktoré už boli testované.

4.2.4.2.2 Výkon

V tejto sekcii môžete meniť počet nezávislých vlákien kontroly, ktoré môžu byť naraz použité. Použitie viacerých vlákien na systémoch s viacerými procesormi môže zvýšiť rýchlosť kontroly. Pre čo najvhodnešie optimalizovanie výkonu odporúčame použiť toľko skenovacích jadier Threatsense koľko použijeme skenovacíh vlákien.

Možnosť **Časový limit odozvy (v sekundách):** definuje maximálny časový úsek, v rámci ktorého vlákno čaká na ukončenie kontroly správy. Ak nie je skenovanie dokončené v tomto časovom limite, Microsoft Exchange Server odmietne klientovi prístup k správe. Skenovanie pritom nie je prerušené a po jeho dokončení bude každý ďalší pokus klienta o prístup k tejto správe úspešný.

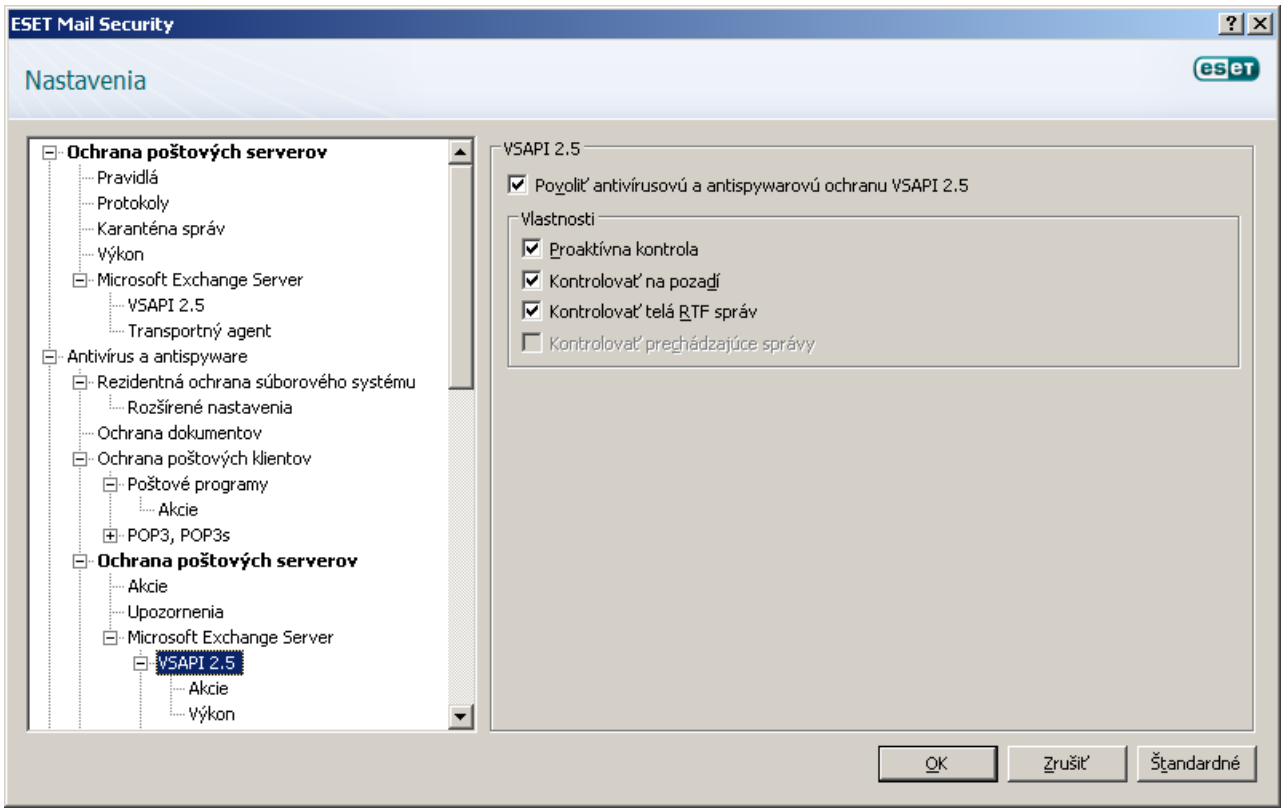


TIP: Pre určenie optimálnej hodnoty pre **Počet vlákien kontroly**, dodávateľ Microsoft Exchange Server odporúča použiť tento vzorec: [počet fyzických procesorov] x 2 + 1.

Poznámka: Výkon sa nezvýši, ak je nastavených viac skenovacích jadier ThreatSense ako skenovacích vlákien.

4.2.4.3 Microsoft Exchange Server 2003 (VSAPI 2.5)

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



Ak je zapnutá možnosť **Proaktívna kontrola**, nové prichádzajúce správy budú kontrolované v tom istom poradí ako boli prijaté.

Možnosť **Kontrolovať na pozadí** umožní kontrolu všetkých správ na pozadí systému. Microsoft Exchange Server si sám určuje, či prebehne kontrola správ okamžite alebo neskôr, a to na základe rôznych faktorov ako sú napríklad momentálne zaťaženie servera, počet aktívnych používateľov, atď. Microsoft Exchange Server si uchováva záznam o kontrolovaných správach a verzii vírusovej databázy použitej pri skenovaní. Ak sa používateľ pokúša otvoriť správu, ktorá nebola skontrolovaná najnovšou verziou vírusových databáz, Microsoft Exchange Server pošle správu najprv na kontrolu ESET Mail Security kým ju umožní otvoriť vo Vašom poštovom programe.
Kedže kontrola na pozadí systému môže zvýšiť nároky na systém (kontrola prebieha po každej aktualizácii vírusovej databázy), odporúčame Vám používať plánovanú kontrolu mimo pracovného času. Plánovanú kontrolu na pozadí môžete nastaviť pridaním úlohy v Plánovači. Ak zadefinujete úlohu na vykonanie kontroly na pozadí môžete určiť čas spustenia, počet opakovaní a množstvo iných parametrov dostupných v Plánovači. Po naplánovaní úlohy, sa táto zobrazí v zozname naplánovaných úloh, v ktorom ju tiež môžete upravovať, vymazať, alebo ju dočasne deaktivovať.

Ak chcete aby boli kontrolované správy s obyčajným textom, označte možnosť **Kontrolovať telá textových správ**.

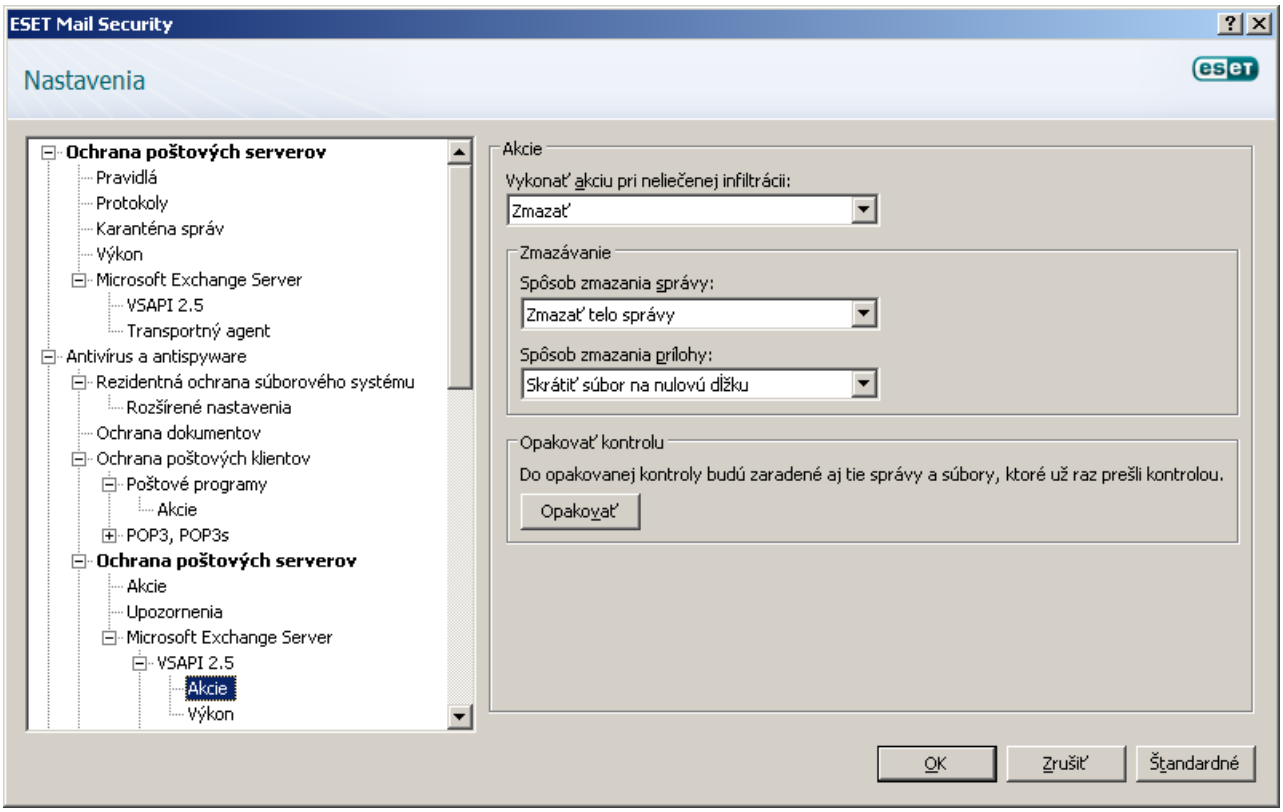
Ak povolíte možnosť **Kontrolovať telá RTF správ**, zapne sa kontrola tiel RTF správ. Aj telá RTF správ môžu obsahovať vírusy.

Možnosť **Kontrolovať prechádzajúce správy** zapne funkcionalitu, ktorá skontroluje aj správy, ktoré sa neukladajú na lokálnom Microsoft Exchange Serveri, ale sú cez neho len doručované iným poštovým serverom. Ak je zapnutá kontrola prechádzajúcich správ ESET Mail Security ich tiež skontroluje. Táto možnosť je dostupná iba ak je vypnutý transportný agent.

Poznámka: VSAPI neskenuje telá textových správ.

4.2.4.3.1 Akcie

V tejto časti môžete nastaviť akcie na vykonanie v prípade, že správa a/alebo príloha bola vyhodnotená ako infikovaná.



Pole **Vykonať akciu pri neliečenej infiltrácii** určí, či sa škodlivý obsah zablokuje alebo sa vymaže celá správa. Táto akcia bude použitá len ak sa pri automatickom liečení (ako je definované v **Nastavenie parametrov skenovacieho jadra ThreatSense > Liečenie**) nepodarilo správu vyliečiť.

Možnosť **Spôsob zmazania tela správy** ponúka alternatívu, ktorá spočíva v zmazaní tela správy, alebo ďalšiu, ktorá prepíše telo správy informáciou o vykonanej akcii.

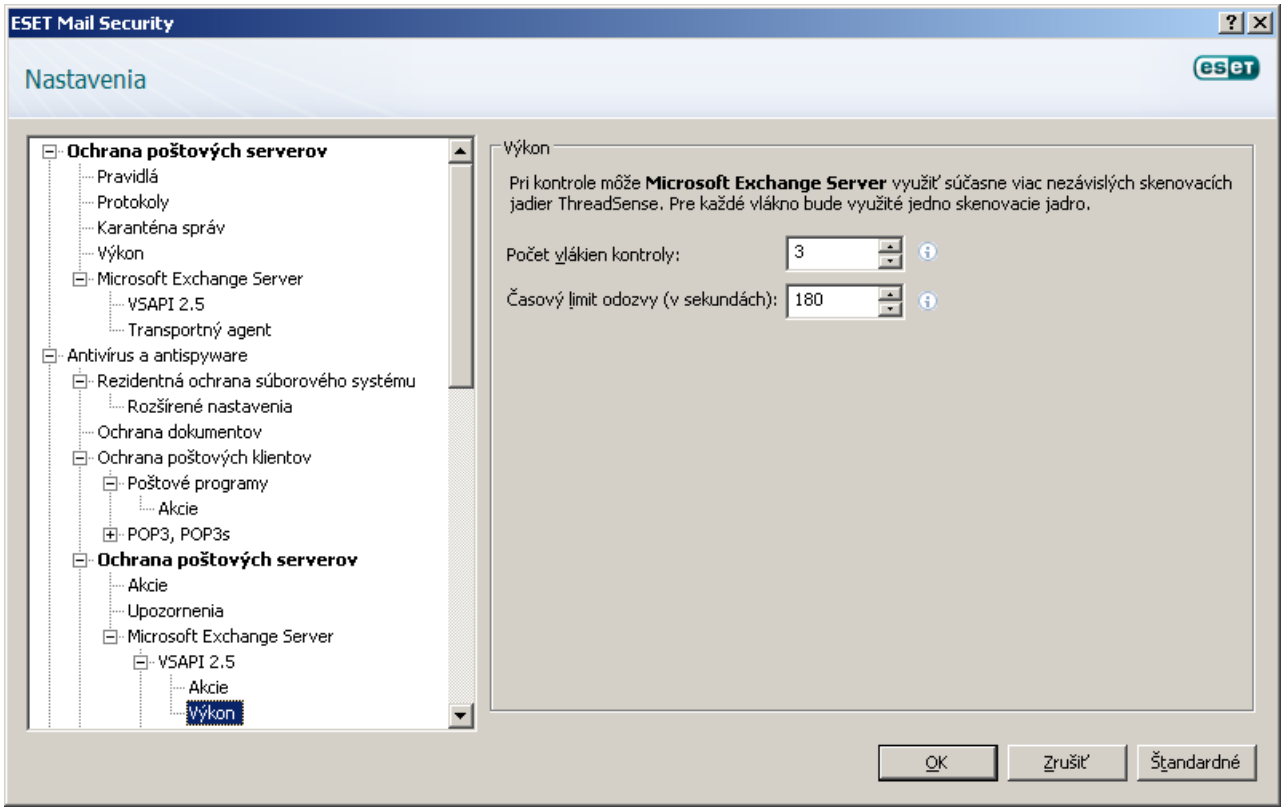
Spôsob zmazania prílohy určuje, či sa vymaže celá správa, alebo sa redukuje veľkosť prílohy na nulu, alebo sa infikovaný súbor nahradí informáciou o vykonanej akcii.

Kliknutím na **Opakovať kontrolu** program znovu prekontroluje aj správy, ktoré už boli testované.

4.2.4.3.2 Výkon

V tejto sekcii môžete meniť počet nezávislých vlákien kontroly , ktoré môžu byť naraz použité. Použitie viacerých vlákien na systémoch s viacerými procesormi môže zvýšiť rýchlosť kontroly. Pre čo najvhodnešie optimalizovanie výkonu odporúčame použiť toľko skenovacích jadier Threatsense koľko použijeme skenovacích vlákien.

Možnosť **Časový limit odozvy (v sekundách):** definuje maximálny časový úsek, v rámci ktorého vlákno čaká na ukončenie kontroly správy. Ak nie je skenovanie dokončené v tomto časovom limite, Microsoft Exchange Server odmietne klientovi prístup k správe. Skenovanie pritom nie je prerušené a po jeho dokončení bude každý ďalší pokus klienta o prístup k tejto správe úspešný.

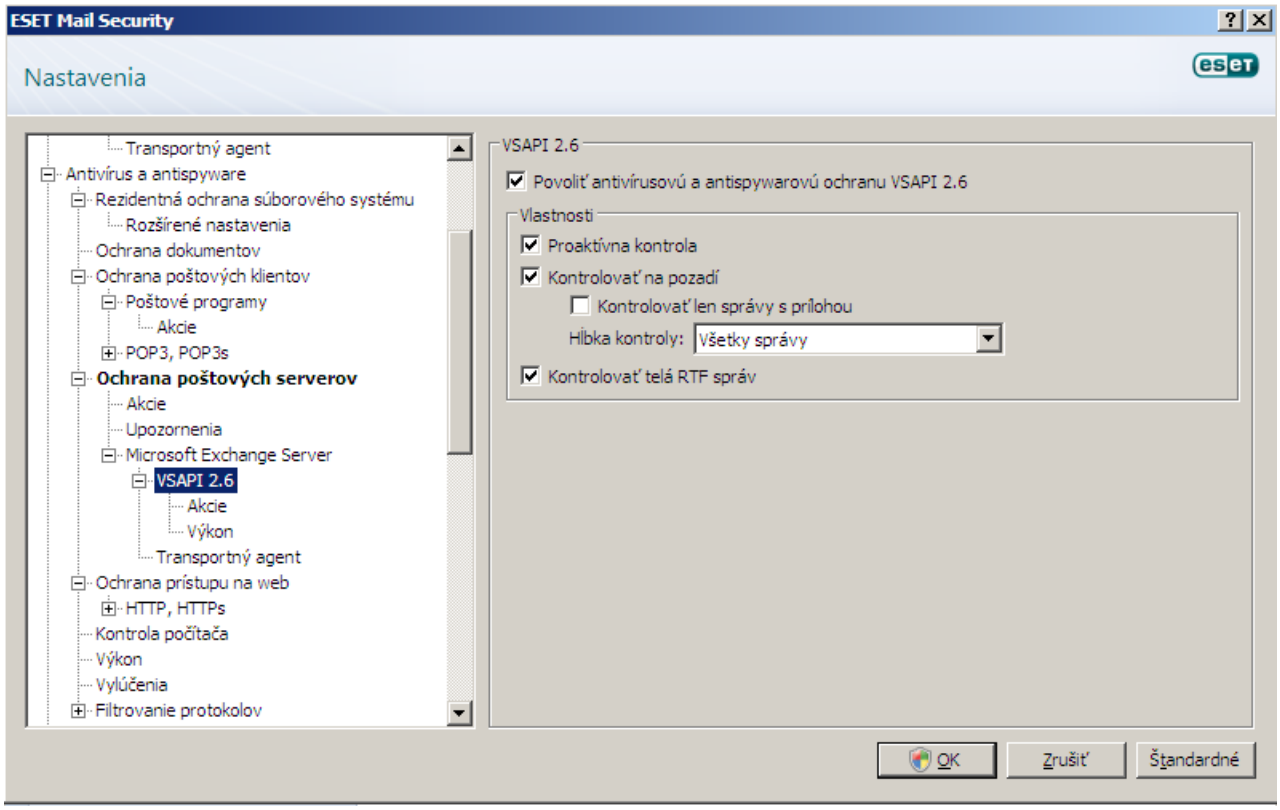


TIP: Pre určenie optimálnej hodnoty pre **Počet vlákien kontroly**, dodávateľ Microsoft Exchange Server odporúča použiť tento vzorec: [počet fyzických procesorov] x 2 + 1.

Poznámka: Výkon sa nezvýši, ak je nastavených viac skenovacích jadier ThreatSense ako skenovacích vlákien.

4.2.4.4 Microsoft Exchange Server 2007/2010 (VSAPI 2.6)

Táto verzia Microsoft Exchange Server obsahuje VSAPI verziu 2.6.



Ak je zapnutá možnosť **Proaktívna kontrola,** nové prichádzajúce správy budú kontrolované v tom istom poradí, v akom boli prijaté.

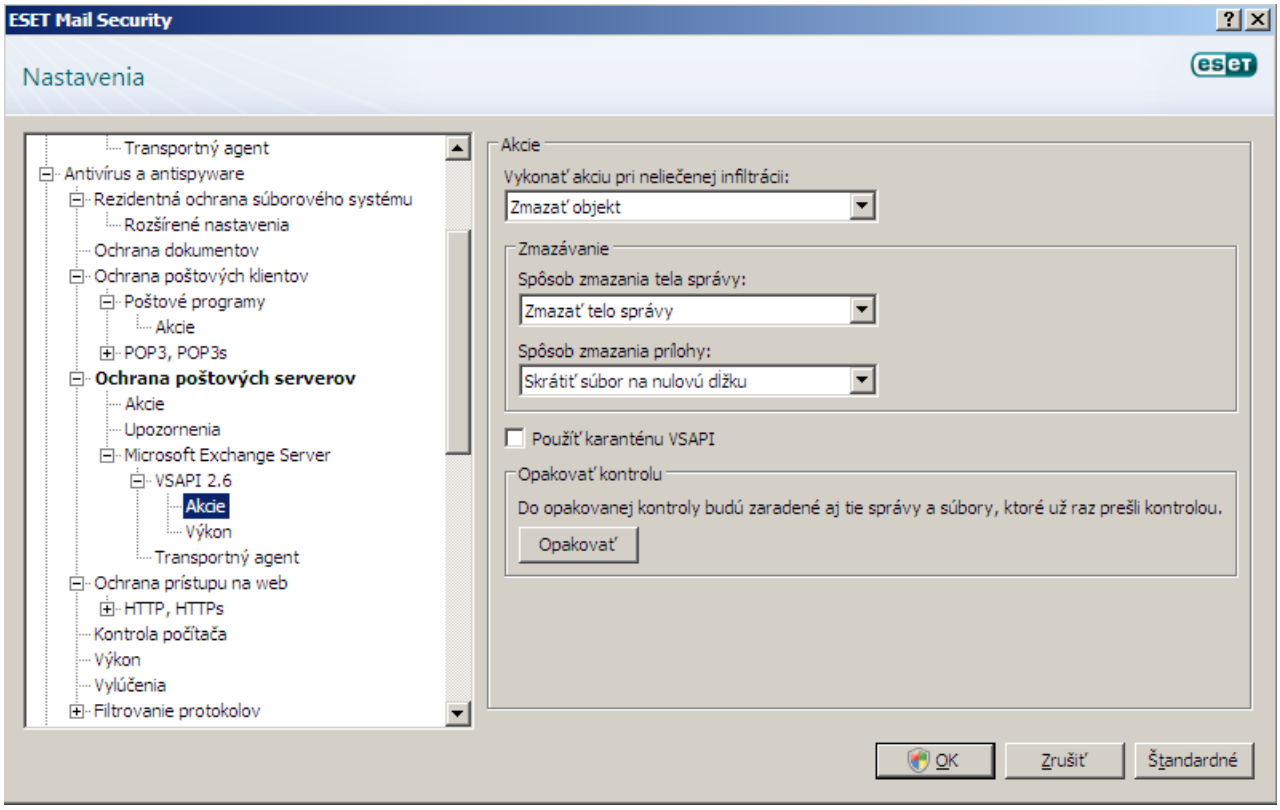
Možnosť **Kontrolovať na pozadí** umožní kontrolu všetkých správ na pozadí systému. Microsoft Exchange Server si

sám určuje, či prebehne kontrola správ okamžite alebo neskôr, a to na základe rôznych faktorov ako sú napríklad momentálne zaťaženie servera, počet aktívnych používateľov, atď. Microsoft Exchange Server si uchováva záznam o kontrolovaných správach a verzii vírusovej databázy použitej pri skenovaní. Ak sa používateľ pokúša otvoriť správu, ktorá nebola skontrolovaná najnovšou vírusovou databázou, Microsoft Exchange Server pošle správu najprv na kontrolu ESET Mail Security kým ju umožní otvoriť vo Vašom poštovom programe. Môžete takisto zvoliť možnosť **Kontrolovať len správy s prílohou** a filtrovať ich podľa času kedy boli prijaté.
Kedže kontrola na pozadí systému môže zvýšiť nároky na systém (kontrola prebieha po každej aktualizácii vírusovej databázy), odporúčame Vám používať plánovanú kontrolu mimo pracovného času. Plánovanú kontrolu na pozadí môžete nastaviť pridaním úlohy v Plánovači. Ak zadefinujete úlohu na vykonanie kontroly na pozadí, môžete určiť čas spustenia, počet opakovaní a množstvo iných parametrov dostupných v Plánovači. Po naplánovaní úlohy sa táto zobrazí v zozname naplánovaných úloh, v ktorom ju tiež môžete upravovať, vymazať, alebo ju dočasne deaktivovať.

Ak povolíte možnosť **Kontrolovať telá RTF správ** zapne sa kontrola tiel RTF správ. Aj telá RTF správ môžu obsahovať vírusy (makrovírusy).

4.2.4.4.1 Akcie

V tejto časti môžete nastaviť akcie na vykonanie v prípade, že správa a/alebo príloha bola vyhodnotená ako infikovaná.



Pole **Vykonať akciu pri neliečenej infiltrácii** určí, či sa škodlivý obsah zablokuje alebo sa vymaže celá správa. Táto akcia bude použitá len ak sa pri automatickom liečení (ako je definované v **Nastavenie parametrov skenovacieho jadra ThreatSense > Liečenie**) nepodarilo správu vyliečiť.

Možnosť **Spôsob zmazania tela správy** ponúka alternatívu, ktorá spočíva v zmazaní tela správy, alebo prepísaní tela správy informáciou o vykonanej akcii.

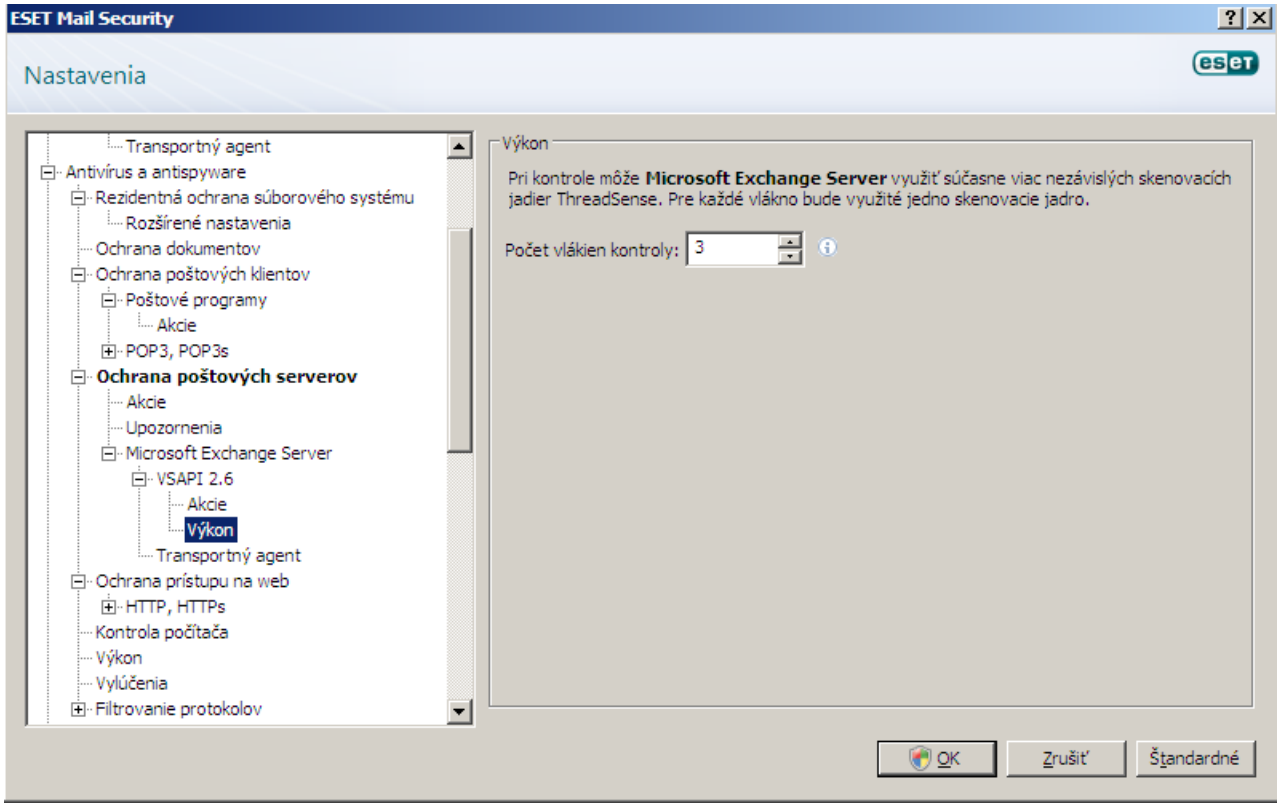
Spôsob zmazania prílohy určuje, či sa vymaže celá správa, alebo sa redukuje veľkosť prílohy na nulu, alebo sa infikovaný súbor nahradí informáciou o vykonanej akcii.

Ak je zapnutá možnosť **Použiť karanténu VSAPI**, infikované správy sa budú ukladať do karantény poštového servera. Tu je potrebné upozorniť na fakt, že toto je serverom spravovaná karanténa a nie karanténa klienta, ani poštový priečinok karantény. Infikované správy uložené v karanténe poštového servera nie sú dostupné, kým nie sú vyliečené pomocou novo aktualizovanej vírusovej databázy.

Kliknutím na **Opakovať kontrolu** program znovu prekontroluje aj správy, ktoré už boli testované.

4.2.4.4.2 Výkon

V tejto sekcii môžete meniť počet nezávislých vlákien kontroly, ktoré môžu byť naraz použité. Použitie viacerých vlákien na systémoch s viacerými procesormi môže zvýšiť rýchlosť kontroly. Pre čo najvhodnešie optimalizovanie výkonu odporúčame použiť toľko skenovacích jadier Threatsense koľko použijeme skenovacích vlákien.

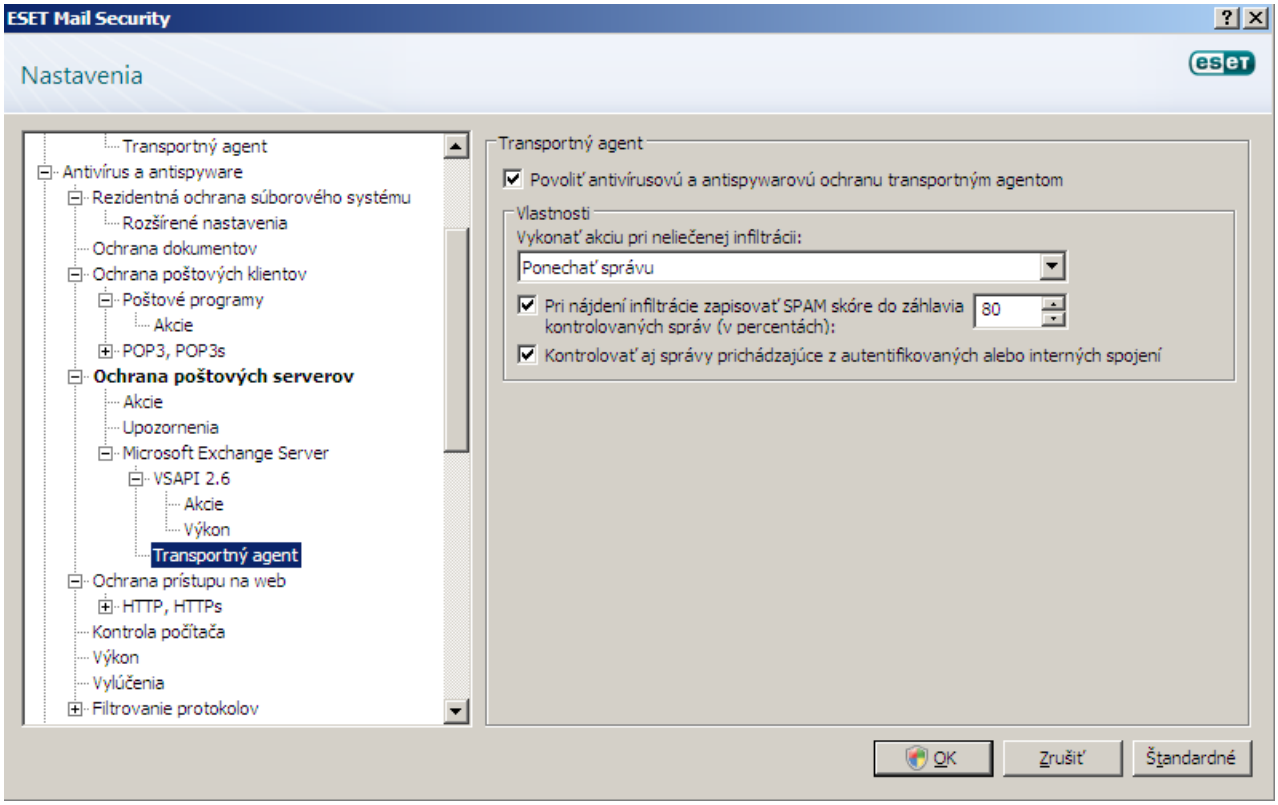


TIP: Pre určenie optimálnej hodnoty pre **Počet vlákien kontroly**, dodávateľ Microsoft Exchange Server odporúča použiť tento vzorec: [počet fyzických procesorov] x 2 + 1.

Poznámka: Výkon sa nezvýši, ak je nastavených viac skenovacích jadier ThreatSense ako skenovacích vlákien.

4.2.5 Transportný Agent

V tejto časti môžete zapnút antivírusovú a antispywarovú ochranu transportným agentom. Transportný agent pre Microsoft Exchange Server 2007 a vyššie sa dá nainštalovať iba v prípade, že server je v jednej z týchto dvoch rolí: *Edge Transport* alebo *Hub Transport*.



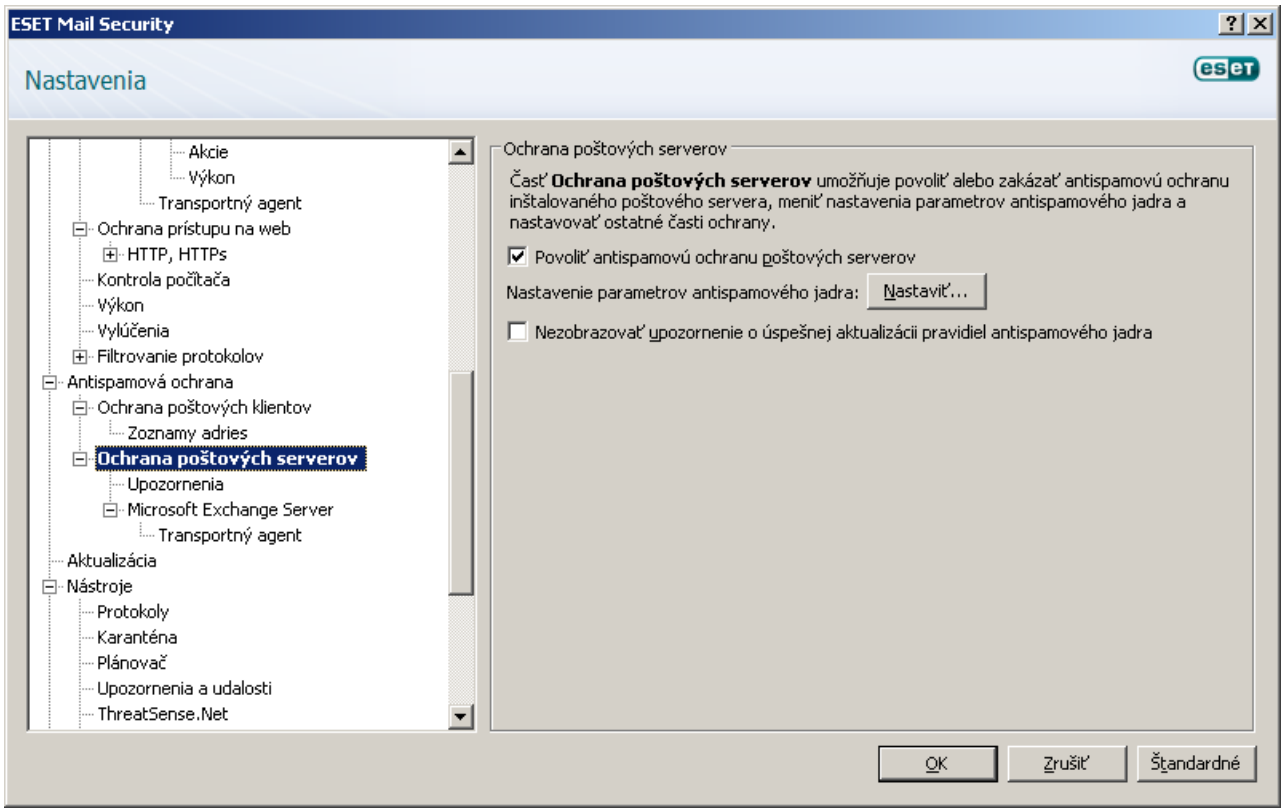
Ak sa správa nedá vyliečiť, môžete ju vymazať, presunúť do karantény, alebo zachovať.

Ak bola nájdená infiltrácia, môžete kontrolovanej správe pripísať spam skóre, ktorého hodnotu udávate v percentách. Keďže botnety sú dnes absolútne majoritným odosielateľom infikovanej pošty, správy posielané týmto spôsobom môžu byť klasifikované ako spam. Aby táto funkcionalita mohla správne fungovať, voľba **Zapisovať stupeň nevyžiadanej pošty (SCL) do záhlavia kontrolovaných správ podľa hodnoty SPAM skóre** musí byť zapnutá (pod **Ochrana poštových serverov > Microsoft Exchange Server > Transportný agent**).

Takisto môžete zapnúť kontrolu pre správy doručované z autentifikovaných zdrojov alebo lokálnych serverov.

4.3 Nastavenia antispamu

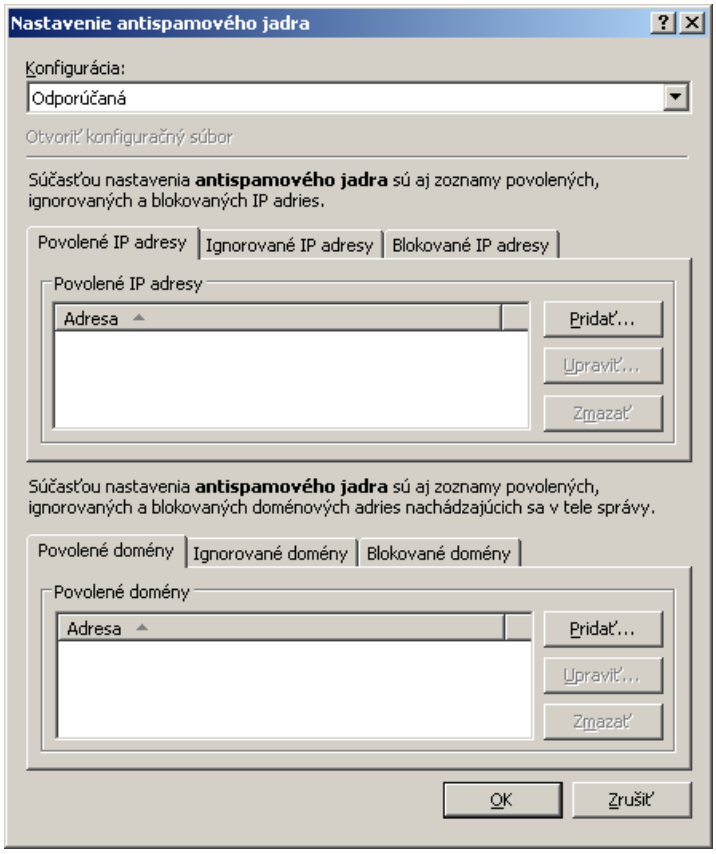
V sekcii **Ochrana poštových serverov** môžete zapnúť ochranu proti spamu na vašom poštovom serveri, konfigurovať nastavenia parametrov antispamového jadra a ďalších úrovní ochrany.



4.3.1 Nastavenia parametrov antispamového jadra

Môžete si vybrať jeden z prednastavených profilov konfigurácie (**Odporúčaná, Maximálna presnosť, Maximálna rýchlosť, Vlastná**). Zoznam profilov sa nahrá z antispamového modulu.

Nastavenie **Odporúčaná** v sebe spája odporúčané nastavenia v rovnovážnom vzťahu medzi úrovňou bezpečnosti a záťažou kladenou na systém.
Nastavenie **Maximálna presnosť** sa zameriava výhradne na bezpečnosť poštového servera. Toto nastavenie spotrebuje viac systémových zdrojov ako Odporúčaná konfigurácia.
Nastavenie **Maximálna rýchlosť** optimalizuje parametre (aj vypínaním určitých funkcionalít kontroly) modulu tak, aby bola spotreba systémových zdrojov čo najnižšia.
Nastavenie **Vlastná > Otvoriť konfiguračný súbor** umožní používateľovi upraviť súbor spamcatcher.conf. Túto možnosť odporúčame len pre pokročilých používateľov. Podrobnosti nájdete v kapitole Konfiguračný súbor 42.



V záložke **Povolené IP adresy** môžete pridávať IP adresy, ktoré majú mať štatút povolené, t.j. ak prvá neignorovaná IP adresa v Prijatých hlavičkách súhlasí s hociktorou adresou v tomto zozname, správe sa pridelí skóre 0 a viac sa už nekontroluje.
V záložke **Ignorované IP adresy** môžete pridať IP adresy, ktoré budú ignorované pri RBL (Real-time Blackhole List) kontrolách. Tu by sa mali nachádzať všetky IP adresy firewallu, ktoré nie sú priamo dostupné z Internetu. Pridaním takýchto adries zabránite nepotrebným kontrolám a umožníte systému identifikovať naozaj sa pripájajúce IP adresy. Interné IP adresy sú vynechávané programom automaticky (192.168.x.y and 10.x).
V záložke **Blokované IP adresy** môžete pridávať IP adresy, ktoré by mali byť blokované, t.j. ak akákoľvek neignorovaná IP adresa v Prijatých hlavičkách súhlasí s hociktorou adresou v tomto zozname, správe sa pridelí skóre 100 a už neprebiehajú žiadne ostatné kontroly.

V záložke **Povolené domény** môžete pridávať domény použité v telách správ, ktoré majú byť vždy prijaté.
V záložke **Ignorované domény** môžete pridávať domény použité v telách správ, ktoré majú byť vždy vylúčené z kontrol DNSBL a MSBL a ignorované.
V záložke **Blokované domény** môžete pridávať domény použité v telách správ, ktoré majú byť vždy blokované.

4.3.1.1 Konfiguračný súbor

Konfiguračný súbor *spamcatcher.conf* obsahuje množstvo ďalších nastavení, ktoré nie sú dostupné cez grafické rozhranie ESET Mail Security, avšak je možné ich meniť práve prostredníctvom tohto súboru. Nastavenia v *spamcatcher.conf* sú prehľadne štrukturované a majú svoju formu. Každé z nastavení obsahuje tieto položky:

Name - názov nastavenia
Arguments - hodnoty, ktoré môže nastavenie nadobúdať a formát v akom sa zapisujú
Default - štandardná hodnota nastavenia
Description - podrobný opis/vysvetlenie k nastaveniu

Prázdne riadky, ako aj riadky začínajúce znakom # sú ignorované.

Zoznam najdôležitejších nastavení súboru *spamcatcher.conf*:

Názov nastavenia	Detaily
approved_ip_list	Zoznam povolených IP adries. Nie je potrebné ho zadávať do *spamcatcher.conf*, nastavuje sa priamo cez grafické rozhranie programu (viď kapitola Nastavenia parametrov antispamového jadra 41).

blocked_ip_list	Zoznam blokovaných IP adries. Nie je potrebné ho zadávať do *spamcatcher.conf*, nastavuje sa priamo cez grafické rozhranie programu (viď kapitola Nastavenia parametrov antispamového jadra 41).
ignored_ip_list	Zoznam ignorovaných IP adries. Nie je potrebné ho zadávať do *spamcatcher.conf*, nastavuje sa priamo cez grafické rozhranie programu (viď kapitola Nastavenia parametrov antispamového jadra 41).

rbl_list	Zoznam Realtime Blackhole serverov, ktoré majú byť použité pri vyhodnocovaní správy. RBL požiadavka spočíva v kontrole, či sa konkrétna IP adresa nachádza na danom RBL serveri. Kontrolované sú IP adresy nachádzajúce sa v sekciách Received: v hlavičke emailu.
	Formát zápisu je:
	`rbl_list=server:response:offset,server2:response2:offset2,...`
	
	Význam jednotlivých parametrov:
	1) server - meno RBL servera
	2) response - odpoveď RBL servera v prípade ak sa na ňom daná IP adresa nachádza (štandardné odpovede sú 127.0.0.2, 127.0.0.3, 127.0.0.4., atď.). Je to nepovinný parameter a ak nie je definovaný, do úvahy sa berú všetky odpovede.
	3) offset - hodnota od 0 do 100. Ovplyvňuje celkové spam skóre správy. Štandardná hodnota je 100, čo znamená, že v prípade pozitívneho nálezu je správe pridelené spam skóre 100 a je tak vyhodnotená ako spam. Negatívne hodnoty uberajú z celkového spam skóre správy. Hodnotu 0 očakávajte tiež v prípadoch, že ide o správy od odosieľateľov zo súboru *approvedsenders* a hodnotu 100 zasa ak sa jedná o správy odosielateľov zo súboru *blockedsenders* (viď nižšie).
	
	Príklad 1:
	`rbl_list=ent.adbl.org`
	RBL kontrola prebieha voči serveru `ent.adbl.org` a v prípade pozitívneho nálezu je správe priradený štandardný offset 100, čím je správa jednoznačne označená za spam.
	
	Príklad 2:
	`rbl_list=ent.adbl.org::60`
	RBL kontrola prebieha voči serveru `ent.adbl.org` a v prípade pozitívneho nálezu je správe priradený offset 60, čo zvyšuje celkové spam skóre správy
	
	Príklad 3:
	`rbl_list=bx9.dbl.com::85, list.dnb.org:127.0.0.4:35, req.gsender.org::-75`
	RBL kontrola prebieha voči zadefinovaným serverom (zľava doprava). V prípade pozitívneho nálezu na `bx9.dbl.com` je použitý offset 85. V prípade pozitívneho nálezu na `list.dnb.org` a odpovedi `127.0.0.4` je použitý offset 35. V prípade inej odpovedi ako 127.0.0.4 nie je offset aplikovaný. V prípade pozitívneho nálezu na `req.gsender.org` sa spam skóre zníži o 75 bodov (záporná hodnota).

rbl_max_ips	Maximálny počet IP adries, ktoré sa posielajú na kontrolu RBL serveru. Celkový počet RBL požiadaviek pritom pozostáva z počtu IP adries nachádzajúcich sa v sekciách Received: v hlavičke emailu (až do limitu definovaného v rbl_maxcheck_ips) vynásobeného počtom RBL serverov definovanom v rbl_list. Hodnota 0 znamená kontrolu neobmedzeného počtu IP adries. IP adresy nachádzajúce sa v ignored_ip_list (t.j. v zozname **Ignorované IP adresy** v nastaveniach ESET Mail Security) sa do limitu rbl_max_ips nezapočítavajú. Toto nastavenie sa aplikuje iba vtedy, ak je rbl_list aktivovaný (obsahuje aspoň jeden server).
approved_domain_list	Ide o zoznam domén a IP adries nachádzajúcich sa v tele emailu, ktoré majú byť povolené. Nepoužívať na whitelistovanie mailov podľa domény odosieľatela !
blocked_domain_list	Zoznam domén a IP adries nachádzajúcich sa v tele emailu, ktoré majú byť vždy blokované. Nejde o blacklist na adresu odosieľateľa ! Nie je potrebné ho zadávať do *spamcatcher.conf*, nastavuje sa priamo cez grafické rozhranie programu (viď kapitola Nastavenia parametrov antispamového jadra 41).
ignored_domain_list	Zoznam domén nachádzajúcich sa v tele emailu, ktoré majú byť vždy vylúčené z DNSBL kontroly a ignorované. Nie je potrebné ho zadávať do *spamcatcher.conf*, nastavuje sa priamo cez grafické rozhranie programu (viď kapitola Nastavenia parametrov antispamového jadra 41).
dnsbl_list	Zoznam DNSBL serverov voči ktorým sa majú kontrolovať domény a IP adresy nachádzajúce sa v tele emailu. Formát zápisu: `dnsbl_list=server:response:offset,server2:response2:offset2,...`

	Význam jednotlivých parametrov:
	1) server - meno DNSBL servera
	2) response - odpoveď DNSBL servera v prípade ak sa na ňom daná IP adresa/doména nachádza (štandardné odpovede sú 127.0.0.2, 127.0.0.3, 127.0.0.4., atď.). Je to nepovinný parameter a ak nie je definovaný, do úvahy sa berú všetky odpovede.
	3) offset - hodnota od 0 do 100. Ovplyvňuje celkové spam skóre správy. Štandardná hodnota je 100, čo znamená, že v prípade pozitívneho nálezu je správe pridelené spam skóre 100 a je tak vyhodnotená ako spam. Negatívne hodnoty uberajú z celkového spam skóre správy. Hodnotu 0 očakávajte tiež v prípadoch, že ide o správy od odosieľateľov zo súboru *approvedsenders* a hodnotu 100 zasa ak sa jedná o správy odosielateľov zo súboru *blockedsenders* (viď nižšie).
	
	Kontrola prostredníctvom DNSBL môže výrazne negatívne ovplyvniť výkon, pretože každá doména/IP adresa z tela správy je kontrolovaná voči všetkým zadefinovaným DNSBL serverom a každá takáto kontrola si vyžaduje požiadavku voči DNS serveru. Stratu výkonu je možné zmierniť nasadením DNS cache servera pre tento účel. Z dôvodu výkonu sú z kontroly vynechané non-routable IP adresy (10.x.x.x, 127.x.x.x, 192.168.x.x).
	
	Príklad 1:
	`dnsbl_list=ent.adbl.org`
	DNSBL kontrola prebieha voči serveru `ent.adbl.org` a v prípade pozitívneho nálezu je správe priradený štandardný offset 100, čím je správa jednoznačne označená za spam.
	
	Príklad 2:
	`dnsbl_list=ent.adbl.org::60`
	DNSBL kontrola prebieha voči serveru `ent.adbl.org` a v prípade pozitívneho nálezu je správe priradený offset 60, čo zvyšuje celkové spam skóre správy
	
	Príklad 3:
	`dnsbl_list=bx9.dbl.com::85, list.dnb.org:127.0.0.4:35, req.gsender.org::-75`
	DNSBL kontrola prebieha voči zadefinovaným serverom (zľava doprava). V prípade pozitívneho nálezu na `bx9.dbl.com` je použitý offset 85. V prípade pozitívneho nálezu na `list.dnb.org` a odpovedi `127.0.0.4` je použitý offset 35. V prípade inej odpovedi ako 127.0.0.4 nie je offset aplikovaný. V prípade pozitívneho nálezu na `req.gsender.org` sa spam skóre zníži o 75 bodov (záporná hodnota).

home_country_list	Zoznam krajín, ktoré budú považované za "domáce". Správy smerované cez krajinu, ktorá nie je v tomto zozname bude prísnejšie hodnotená (pridaním vyššieho spam skóre). Krajiny sa do zoznamu zadávaju ako dvojpísmenkový kód, podľa normy ISO 3166.
home_language_list	Zoznam preferovaných jazykov - t.j. najpoužívanejších jazykov vo vašich emailových správach. Takéto správy sú z pohľadu spam skóre menej prísne hodnotené. Jazyky sa do zoznamu zadávajú ako dvojpísmenkový kód, podľa normy ISO 639.
custom_rules_list	Umožňuje zadefinovať vlastné zoznamy pravidiel, pričom tieto sú uložené v osobitnom súbore/súboroch. Pravidlá sa v súbore nachádzajú každé na samostatnom riadku a majú tento formát: **Phrase**, **Type**, **Confidence**, **CaseSensitivity** **Phrase** - môže to byť akýkoľvek text neobsahujúci čiarku (,) **Type** - môže mať tieto hodnoty: SPAM, PHISH, BOUNCE, ADULT, FRAUD. Pokiaľ zadáte akúkoľvek inú hodnotu, automaticky bude použitá hodnota SPAM. Typ SPAM predstavuje frázy vyskytujúce sa v klasických spamových správach (ponúkanie rôznych tovarov). Typ PHISH predstavuje frázy vyskytujúce sa v podvodných správach (phishing), ktorých cieľom je získať od užívateľa citlivé údaje (mená, heslá, číslo kreditnej karty a pod.). Typ BOUNCE predstavuje frázy používané v automatických správach zo serverov - Non-Delivery Notification (typické pri spoofovaní adresy odosieľateľa). Typ ADULT predstavuje frázy typické pre správy s pornografickým obsahom. Typ FRAUD predstavuje frázy vyskytujúce sa v podvodných emailoch (tzv. Scam) ponúkajúcich často rôzne podozrivé bankové operácie (prevody peňazí cez Vaše konto a pod.). Typickým predstaviteľom tohto typu spamu je tzv. Nigérijský spam. **Confidence** - hodnota od 0 do 100. Vo vzťahu k Type určuje pravdepodobnosť s akou fráza patrí do danej kategórie. Ak je napríklad Type PHISH a Confidence 90, znamená to, že daná fráza sa s veľkou pravdepodobnosťou vyskytuje v správach typu phishing. Čím vyššia je hodnota Confidence, tým väčší dopad má na celkové spam skóre správy. Hodnota 100

	predstavuje špeciálny prípad, kedy výsledné spam skóre správy bude tiež 100 a správa tak bude označená ako 100% spam. Podobne pri hodnote 0 bude správa označená ako nie spam. **CaseSensitivity** - hodnota 0 alebo 1. 0 znamená, že Phrase je case insensitive. 1 znamená, že Phrase je case sensitive. Príklady: replica, SPAM, 100, 0 Dear eBay member, PHISH, 90, 1 return to sender, BOUNCE, 80, 0

Ďalšie možnosti blacklistovania/whitelistovania predstavujú súbory *approvedsenders* a *blockedsenders* (bez koncovky), ktoré sa spolu so súborom *spamcatcher.conf* nachádzajú v adresári C:*Documents and Settings\All Users\Application Data\ESET\ESET Mail Security\MailServer*. Je možné do nich pridať adresy odosielateľov, príp. iba domény, pričom súbor *approvedsenders* predstavuje zoznam povolených adries/domén, zatiaľ čo súbor *blockedsenders* predstavuje zoznam blokovaných adries/domén.

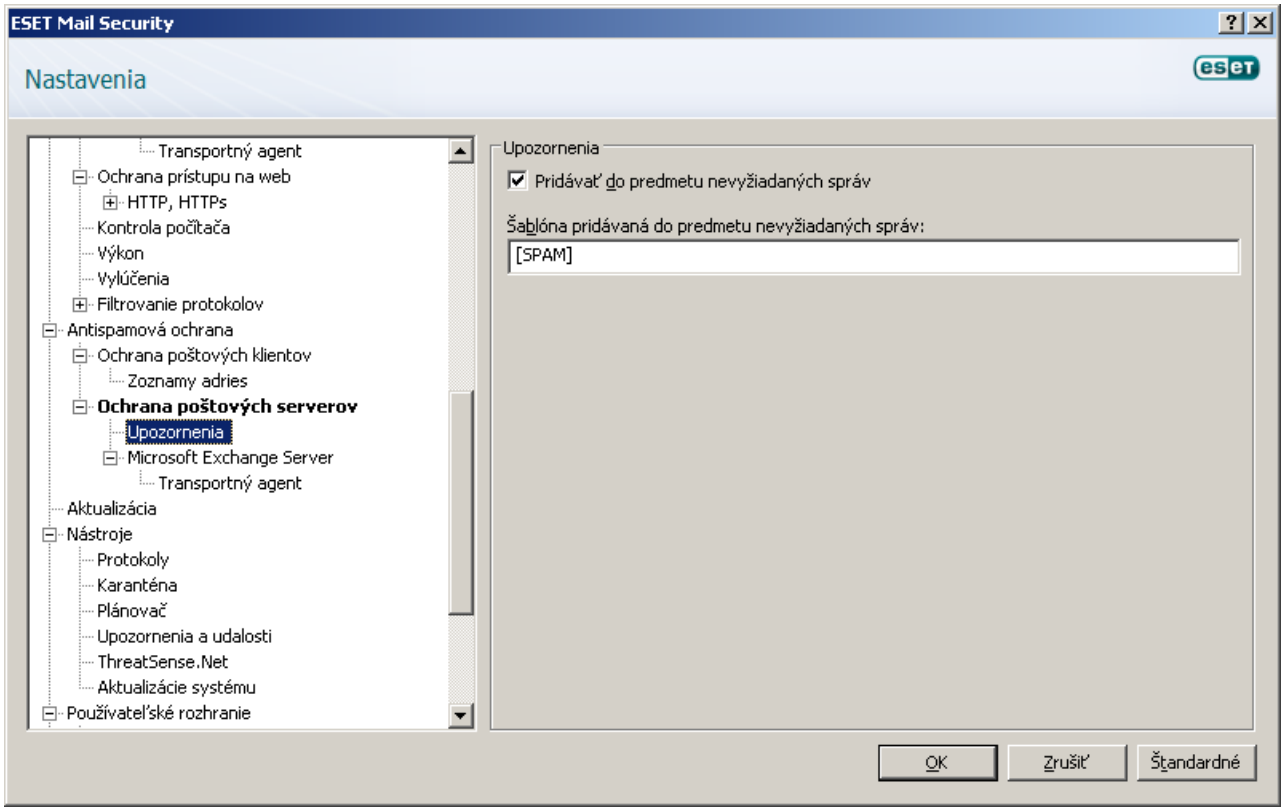
Upozornenie: Keďže adresa odosielateľa býva často falšovaná, použitie súborov *approvedsenders* a *blockedsenders* nie je odporúčaný spôsob whitelistovania/blacklistovania. Spoľahlivejšie je používať zoznamy povolených a blokovaných IP adries. Ak z nejakého dôvodu potrebujete použiť whitelistovanie podľa adresy/domény odosielateľa (súbor *approvedsenders*), mala by byť vždy použitá aj niektorá ďalšia efektívna technológia kontroly (napr. SPF).

Niektoré ďalšie nastavenia:

enable_spf	Táto voľba zapína/vypína kontrolu prostredníctvom Sender Policy Framework. Kontrola spočíva v overení, či je odosielateľ oprávnený odosielať správy z danej domény - na základe zverejnených pravidiel danej domény (domain policy).
enable_all_spf	Táto voľba rozhoduje o tom, či domény, ktoré nie sú v spf_list alebo v Mailshell súbore s pravidlami, môžu obísť SPF kontrolu. Pre správne fungovanie musí byť voľba enable_realtime_spf nastavená na yes.
enable_realtime_spf	Ak je táto voľba zapnutá, pri SPF kontrole sa budú posielať DNS požiadavky v reálnom čase. Môže to mať negatívny vplyv na výkon (zdržanie pri vyhodnocovaní správy).
spf_list	Táto voľba umožňuje ovplyvniť SPF záznam domény prostredníctvom priradenia váhy danému SPF záznamu, čím je možné ovplyvniť celkové spam skóre správy.
spf_*_weight	Hviezdička (asterisk) uprostred predstavuje 14 možných výsledkov z SPF kontroly (viď *spamcatcher.conf* pre viac detailov). Hodnota zadaná v tomto nastavení predstavuje tzv. vyváženie (offset), ktoré sa aplikuje na spam skóre pre jednotlivé typy výsledkov. Ak je napríklad výsledok SPF kontroly "fail", tak sa aplikuje vyváženie z nastavenia spf_fail_weight. Od hodnoty vyváženia potom závisí, či sa celkové spam skóre zvýši alebo zníži.
spf_recursion_depth	Maximálna hĺbka vnorenia (použitie mechanizmu "include"). Podľa normy RFC 4408 je tento limit špecifikovaný na 10 (kvôli zabráneniu Denial-of-Service), avšak niektoré súčasné SPF záznamy toto nespĺňajú a musia používať viac úrovní vnorenia aby bola SPF požiadavka úplne vyhodnotená.
enable_livefeed_sender_repute	Ak je táto voľba vypnutá, SPF informácia z LiveFeed bude ignorovaná.

4.3.2 Upozornenia a udalosti

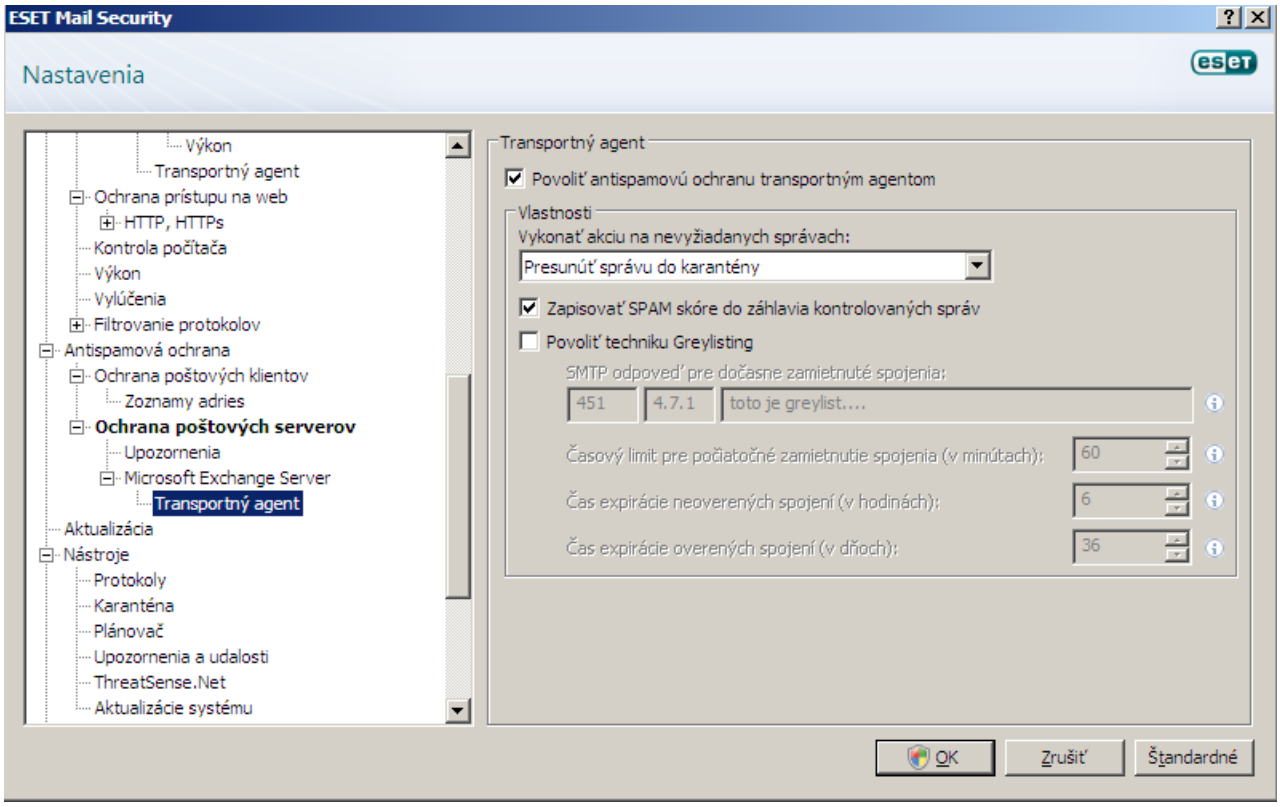
Do predmetu každého e-mailu, ktorý bol prekontrolovaný pomocou ESET Mail Security a označený ako spam môžete pridať vlastnú poznámku. Štandardne sa pridáva poznámka v tvare [SPAM], prípadne si používateľ môže zadefinovať vlastný text.



Poznámka: Pri zostavovaní textu, ktorý sa pridá do predmetu správy môžete použiť aj systémové premenné.

4.3.3 Transportný agent

Tu môžete nastaviť možnosti ochrany proti spamu pomocou transportného agenta.



Poznámka: Transportný agent nie je vo verzii Microsoft Exchange Server 5.5.

So spamovými správami môžete robiť nasledovné:

- Ponechať správu aj napriek tomu, že bola označená ako spam.
- Poslať správu do priečinka karantény.
- Vymazať správu.

Ak chcete aby hlavička správy obsahovala výšku zisteného spamového skóre, zapnite možnosť **Pri nájdení infiltrácie zapisovať SPAM skóre do kontrolovaných správ (v percentách):**

Aktivovaním možnosti **Povoliť techniku Greylisting** zapnete funkcionalitu, ktorá chráni používateľov pre spamom týmto spôsobom: Transportný agent pošle obratom SMTP hodnotu "temporarily rejected", t.j. "dočasne zamietnutá" (prednastavená je 451/4.7.1) na každú prijatú správu, ktorá nepochádza z identifikovaného zdroja. Legitímny server sa pokúsi správu po určitom zdržaní znovu preposlať. Servery odosielajúce spam sa zvyčajne nepokúšajú tieto správy pri neúspešnom doručení znova odoslať, pretože odosielajú tísíce emailových adries naraz a nemajú čas na spätnú kontrolu. Greylisting je ďalšou účinnou vrstvou ochrany pred spamom a nemá žiaden vplyv na hodnotiace schopnosti antispamového modulu.
Pri vyhodnocovaní zdroja správy Greylisting zohľadňuje nastavenia na zoznamoch: **Povolené IP adresy**, **Ignorované IP adresy**, zoznamy **Safe Senders** a **Allow IP** definované na Exchange Serveri, a tiež nastavenie AntispamBypass pre daný mailbox (schránku). Správy z týchto IP adries/Safe Sender zoznamov, resp. správy doručované do schránky so zapnutým AntispamBypass budú z kontroly pomocou metódy Greylisting vynechané.

V poli **SMTP odpoveď pre dočasne zamietnuté spojenia:** sa dá nastaviť dočasná odpoveď poslaná SMTP serveru.

Príklad SMTP odpovede:

Primárny kód odpovede	Doplnkový kód stavu	Popis
451	4.7.1	Požadovaná operácia prerušená: lokálna chyba v procese

Pozor!: Použitie nesprávnej syntaxe v kódoch odpovedí, môže viesť k chybám v ochrane pomocou greylistingu. Jednou z chýb, ktoré by mohli nastať, je napríklad doručovanie spamu klientom, alebo naopak nedoručenie žiadnej zo správ.

Časový limit pre počiatočné zamietnutie spojenia (v minútach) - ak je správa doručená prvýkrát a dočasne zamietnutá, toto nastavenie vymedzuje časový úsek, počas ktorého bude táto správa odmietaná (merané od prvého zamietnutia). Po uplynutí nastaveného času bude správa úspešne prijatá. Najmenšia hodnota, ktorú sem môžete zadať je 1 minúta.
Čas expirácie neoverených spojení (v hodinách): - toto nastavenie určuje minimálny časový interval, počas ktorého zostanú uložené údaje tripletu. Legitímny server musí preposlať želanú správu pred ukončením tejto periódy. Táto hodnota musí byť väčšia ako hodnota **Časový limit pre počiatočné zamietnutie spojenia.**
Čas expirácie overených spojení (v dňoch) - najmenší počet dní, počas ktorých bude uložená informácia o triplete a počas ktorých možno prijímať správy od určitého odosielateľa bez akéhokoľvek zdržania. Táto hodnota musí byť väčšia ako hodnota **Čas expirácie neoverených spojení (v hodnotách):**

Poznámka: Pri zostavovaní SMTP odpovede môžete použiť aj systémové premenné.

4.4 Otázky a odpovede

Otázka: Po nainštalovaní EMSX s antispamom prestali prichádzať e-maily do poštových schránok.
Odpoveď: Ak máte aktivovaný greylisting, ide o normálne správanie. V prvých hodinách prevádzky EMSX môžu e-maily prichádzať až s niekoľkohodinovým oneskorením. V pripade problémov odporúčame greylisting vypnúť, prípadne vhodne nakonfigurovať.

Otázka: Skenuje VSAPI pri kontrole príloh mailových správ iba súbory v prílohe alebo aj telá správ?
Odpoveď: Počínajúc verziou Microsoft Exchange Server 2000 SP2 skenuje VSAPI aj telá správ.®

Otázka: Prečo po vypnutí voľby VSAPI aj naďalej prebieha testovanie správ?
Odpoveď: Zmena nastavení vo VSAPI prebieha asynchrónne, t. j. po požiadavke o zmenu nastavení VSAPI systém čaká, kým budú tieto vyžiadané serverom Microsoft Exchange. Tento cyklický proces prebieha v približne minútových intervaloch. Toto isté samozrejme platí aj pre ostatné nastavenia VSAPI.

Otázka: Môže VSAPI zmazať aj celú správu ak obsahuje infikovanú prílohu?
Odpoveď: Áno, VSAPI dokáže zmazať celú správu. Na to je však najprv potrebné v nastaveniach VSAPI v časti **Akcie**

vybrať možnosť **Zmazať celú správu**. Táto možnosť je dostupná v systémoch Microsoft Exchange Server 2003 a novších. Staršie verzie Microsoft Exchange Server odstraňovanie celých správ nepodporujú.

Otázka: Testuje VSAPI aj odosielané správy?
Odpoveď: Áno, VSAPI testuje aj odosielané správy, ak nemáte vo Vašom mailovom programe nastavený na odosielanie správ iný SMTP server, ako váš Microsoft Exchange Server. Táto funkcionalita je dostupná pre verzie Microsoft Exchange Server 2000 Service Pack 3 a novšie.

Otázka: Je možné cez VSAPI nastaviť text, ktorý sa bude pridávať do každej otestovanej správy, podobne ako to robí transportný agent?
Odpoveď: Pridávanie textu do otestovaných správ cez VSAPI nie je možné, pretože Microsoft Exchange Server túto možnosť nepodporuje.

Otázka: Stáva sa mi, že si niektoré správy nedokážem cez Microsoft Outlook otvoriť. Čím to je?
Odpoveď: S najväčšou pravdepodobnosťou je v nastaveniach VSAPI v časti **Akcie** aktivovaná v roletovom menu **Vykonať akciu pri neliečenej infiltrácii** možnosť **Zablokovať** alebo máte pridané pravidlo s nastavenou akciou **Zablokovať**. Obe z týchto volieb spôsobia, že sa infikovaná správa, alebo správa spadajúca do daného pravidla, označí a Microsoft Exchange Server k nej zablokuje prístup.

Otázka: Čo presne vyjadruje v nastaveniach VSAPI v časti **Výkon** položka **Časový limit odozvy**?
Odpoveď: V prípade, že máte nainštalovaný Microsoft Exchange Server 2000 SP2 alebo vyšší, jedná sa o maximálny čas v sekundách potrebný na dokončenie skenovania pre jedno vlákno pomocou VSAPI. Ak nie je skenovanie dokončené v tomto časovom limite, Microsoft Exchange Server odmietne klientovi prístup k správe. Skenovanie pritom nie je prerušené a po jeho dokončení bude každý ďalší pokus klienta o prístup k tejto správe úspešný. Ak ale máte nainštalovaný Microsoft Exchange Server 5.5 SP3 alebo SP4, hodnota je udávaná v milisekundách a vyjadruje čas za aký sa má klient opätovne pokúšať o prístup k súboru, ktorý mu bol odmietnutý z dôvodu neukončeného skenovania.

Otázka: Aký dlhý môže byť zoznam prípon súborov v jednom pravidle?
Odpoveď: Zoznam prípon súborov v jednom pravidle môže byť dlhý až 255 znakov.

Otázka: Mám vo VSAPI nastavenú možnosť **Testovať na pozadí**. Doteraz sa po každej aktualizácií vírusovej databázy správy na Microsoft Exchange Serveri vždy preskenovali. Po poslednej aktualizácií sa tak ale nestalo. V čom je problém?
Odpoveď: Microsoft Exchange Server si sám určuje, či bude po aktualizácii vírusovej databázy skenovať všetky správy okamžite, alebo či sa kontrola vykoná až pri požiadavke klienta o prístup k danej správe. Microsoft Exchange Server skontroluje každú správu predtým, ako ju doručí do klientovho priečinka prijatých správ.

Otázka: Prečo sa pri prijatí jednej správy môže počítadlo pravidiel zvýšiť aj o viac ako jedna?
Odpoveď: Pravidlá sa porovnávajú so správou pri jej spracovaní Transportným agentom (TA) alebo VSAPI. Ak je povolená kontrola správ prostredníctvom TA aj VSAPI, pri príchode správy sa počítadlo pravidiel môže zvýšiť aj o 2 alebo viac. VSAPI pristupuje k jednotlivým častiam správy (telo, príloha) osobitne, a následne aj pravidlá sa použijú pre každú časť osobitne. Navyše, pravidlá sa aplikujú aj počas kontroly prebiehajúcej na pozadí (napr. pri opakovanom skenovaní ukladacieho priestoru poštovej schránky (mailbox) po každej aktualizácii vírusovej databázy), čo môže takisto prispieť k zvýšeniu stavu počítadla.

Otázka: Je ESET Mail Security kompatibilný s Exchange Intelligent Message Filter (IMF)?
Odpoveď: Áno, ESET Mail Security funguje s IMF. Spôsob spracovania emailov vyhodnotených ako spam je v tejto konfigurácií nasledovný:

- Ak má antispamový modul ESET Mail Security nastavenú akciu **Zmazať správu** (alebo **Presunúť správu do karantény**) a na Exchange IMF je nastavená ľubovolná akcia, vykoná sa akcia, ktorá je nastavená v ESET Mail Security.
- Ak má Antispamový modul ESET Mail Security nastavenú akciu na **Ponechať správu**, potom sa vykoná akcia nastavená na IMF (napr, Delete, Reject, Archive...). Pre správne fungovanie tejto funkcionality na IMF je potrebné, aby voľba **Zapisovať stupeň nevyžiadanej pošty (SCL) do záhlavia kontrolovaných správ podľa hodnoty SPAM skóre** bola zapnutá (pod Ochrana poštových serverov > Microsoft Exchange Server > Transportný agent).

Otázka: Ako docielim, aby Microsoft Outlook ukladal nevyžiadanú poštu do užívateľom zadefinovaného priečinka?
Odpoveď: Pri štandardnom nastavení ESET Mail Security ukladá Microsoft Outlook nevyžiadanú poštu do **Junk E-mail** priečinka. Toto správanie zabezpečuje voľba **Zapisovať SPAM skóre do kontrolovaných správ** (**F5 > Antispamová ochrana > Ochrana poštového servera > Microsoft Exchange Server > Transportný agent**). Ak potrebujeme ukladať nevyžiadanú poštu do iného priečinka, treba urobiť nasledovné:

1) V ESET Mail Security:
   - deaktivovať voľbu **Zapisovať SPAM skóre do záhlavia kontrolovaných správ**,

- nastaviť akciu **Ponechať správu** pre správy označené ako spam,
- nastaviť pridávanie textu do predmetu nevyžiadaných správ, napr. "[SPAM]" (**Antispamová ochrana > Ochrana poštového servera > Upozornenia**).

2) V Microsoft Outlook:
- nastaviť pravidlo, ktoré na základe špecifického textu v predmete správy ("[SPAM]") presunie túto správu do užívateľom zadefinovaného priečinka

Otázka: V štatistikách antispamovej ochrany je veľké množstvo emailov v kategórií **Neskontrolované**. Aké emaily nie sú skenované antispamovou ochranou ?
Odpoveď: Do kategórie **Neskontrolované** sa započítavajú:

- všetky správy skenované v čase, keď bola vypnutá antispamová ochrana
- všetky správy posielané vo vnútri organizácie (tie sú skenované iba antivírusovou ochranou)
- všetky správy posielané do mailboxu, ktorý ma v MS Exchange Serveri nastavený atribút **AntispamBypass**
- všetky správy posielané od odosielateľov nachádzajúcich na zozname **Safe Senders**
- všetky správy posielané zo serverov uvedených vo **Whitelist** zozname (napr.v MS Exchange zoznam **IPAllow**, prípadne v ESET Mail Security zoznam **Povolené IP adresy**)

Otázka: Užívatelia si sťahujú poštu do svojich emailových klientov cez POP3 (mimo MS Exchange Servera), ale samotné poštové schránky (mailboxes) sú na MS Exchange Serveri. Bude tieto emaily kontrolovať ESET Mail Security na vírusy a SPAM ?
Odpoveď: Pri takejto konfigurácií bude ESET Mail Security kontrolovať emaily uložené na MS Exchange Serveri iba na prítomnosť vírusov (prostredníctvom VSAPI). Antispamová kontrola nebude možná, pretože prebieha na úrovni SMTP servera.

Otázka: Je možné ovplyvniť od akej výšky spam skóre bude správa vyhodnotená ako spam ?
Odpoveď: Nie. V súčasnosti je toto skóre pevne stanovené na hodnotu 90, avšak v budúcnosti sa plánuje upraviť program tak, aby bolo možné toto skóre meniť.

Otázka: Kontroluje ESET Mail Security správy antispamovou ochranou ak sú tieto sťahované cez POP3 Connector ?
Odpoveď: Správy sťahované cez POP3 Connector sú kontrolované antispamovou ochranou iba na SBS 2008.