



STUDIJNÍ MATERIÁL PRO TECHNICKOU CERTIFIKACI ESET Server Security, Serverové produkty

ESET Server Security	2
Webové rozhraní	3
ESET Mail Security	4
ESET File Security	4
ESET Gateway Security	4
Linux jako Mirror server	5
Jiná serverová řešení	6
ESET NOD32 pro Exchange Server	6
ESET NOD32 pro Kerio	6
NOD32 pro Lotus Domino	6
NOD32 pro Novell Netware Server	6

ESET Server Security

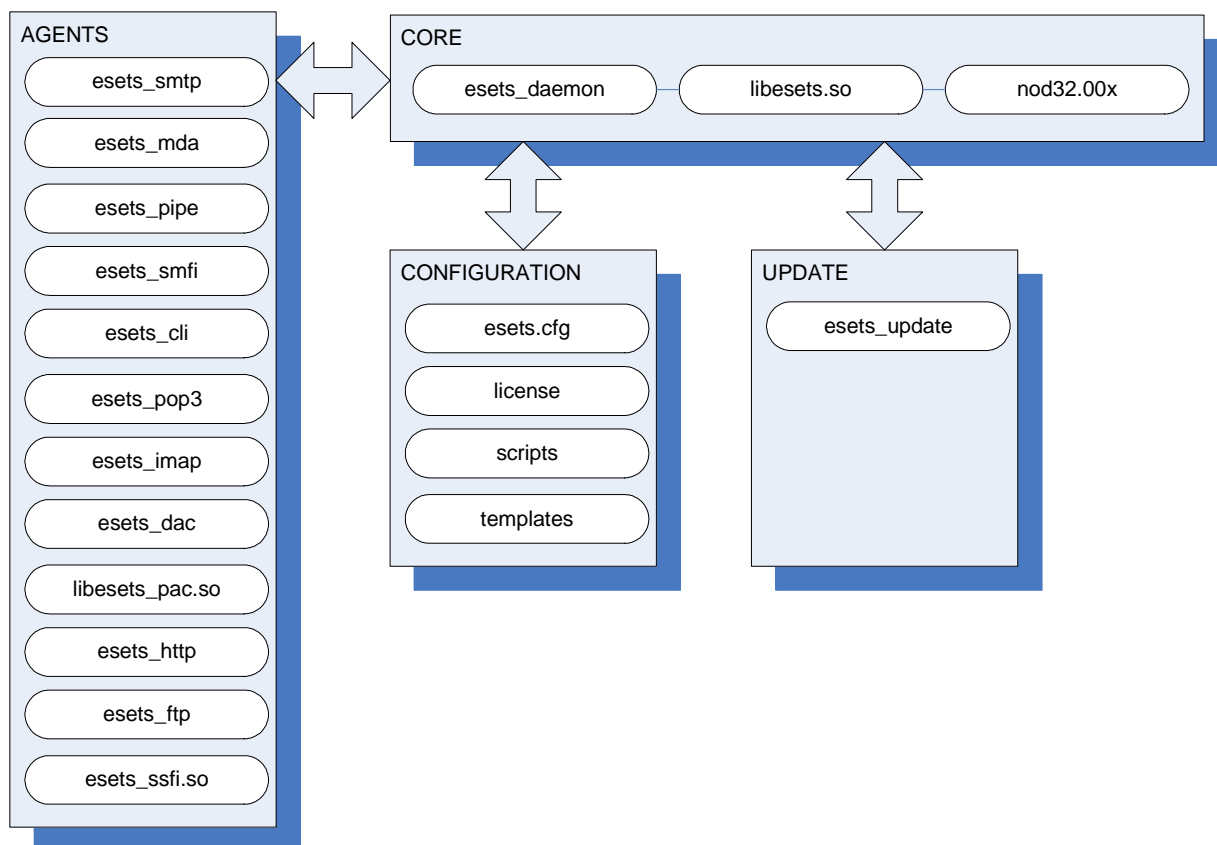
Řada linuxových řešení, zahrnuje:

ESET File Security
ESET Mail Security
ESET Gateway Security

Vlastnosti:

- Plnohodnotná implementace technologie ThreatSense® + ThreatSense.Net
- podpora 32 i 64-bit distribucí, včetně víceprocesorových systémů
- Jádro 2.2 – 2.6 (knihovna GNU Lib C, minimálně 2.2.5)
- Modulární architektura = 1 instalace pro všechny 3 aplikace
- Aktivace pomocí licenčního klíče /každý z produktů má svůj vlastní, aktivní mohou být i všechny 3 na 1 stroji za předpokladu přítomnosti 3 licenčních klíčů/
- dostupnost RPM, DEB, TGZ instalačních balíčků
- možnost definování individuálního nastavení pro mailboxy a domény
- dědění nastavení: globální -> agent -> doména -> schránka (subnet -> IP)
- Instalace skrze průvodce esets_setup

Struktura produktu ESET Server Security:
/licenční klíč odemyká moduly pro konkrétní program/



Webové rozhraní

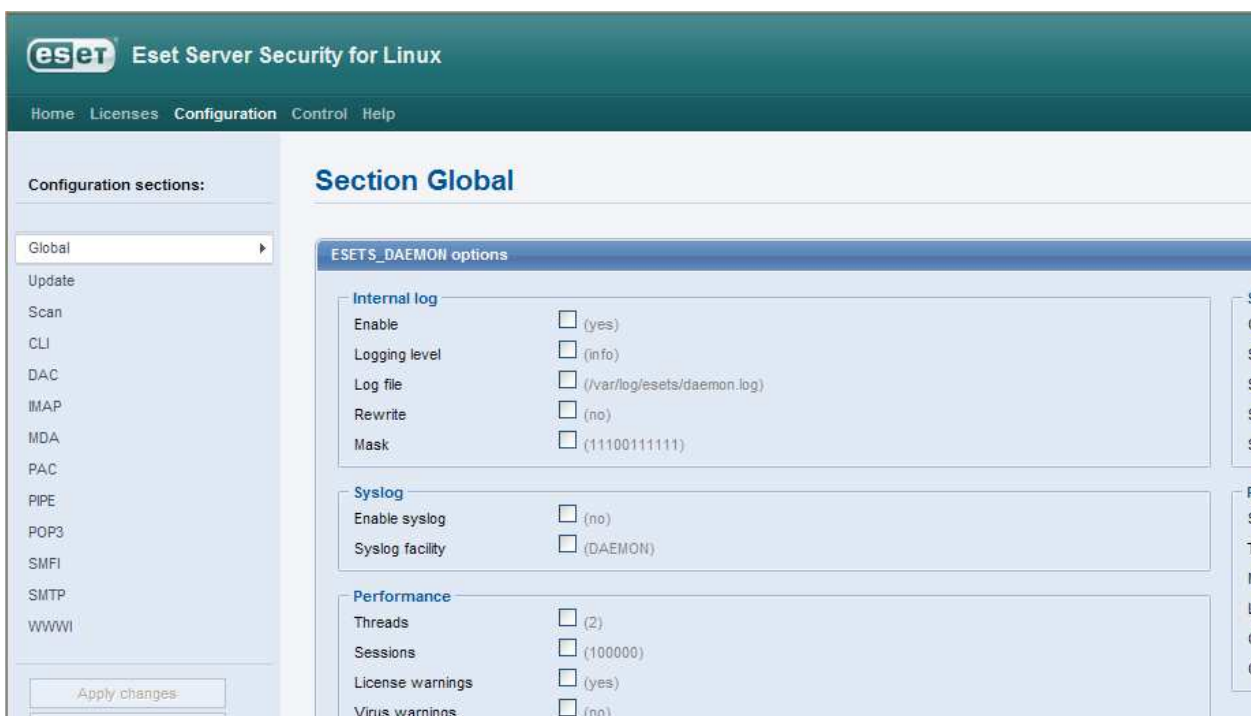
- Vlastní web server, HTTPS komunikace
- Změny za „letu“, kompletní správa nad esets.cfg a lic. klíči
- konfigurace – globální nastavení vs. nastavení jednotlivých modulů
- Vynucení aktualizace a kontroly disku



The screenshot shows the 'Home' page of the Eset Server Security for Linux web interface. The header includes the ESET logo and the product name. A navigation menu contains 'Home', 'Licenses', 'Configuration', 'Control', and 'Help'. The main content area displays system information:

- OS version: Linux 2.4.20-8 i686
- System time: 2007-08-07 16:58:46
- Product version: 2.71.3
- Virus database: 2441 (20070807)
- Licensed products: ESET Mail Security, ESET File Security

Below this information, there is a 'Did you know?' section with the text: 'Use User Configurations to tune scanner setup for given user or group of users.'



The screenshot shows the 'Configuration' page of the Eset Server Security for Linux web interface. The header is identical to the Home page. The left sidebar shows 'Configuration sections:' with a dropdown menu set to 'Global' and a list of other sections: Update, Scan, CLI, DAC, IMAP, MDA, PAC, PIPE, POP3, SMFI, SMTP, and WWWI. An 'Apply changes' button is at the bottom of the sidebar.

The main content area is titled 'Section Global' and contains 'ESETS_DAEMON options' grouped into three sections:

- Internal log**
 - Enable: (yes)
 - Logging level: (info)
 - Log file: (/var/log/esets/daemon.log)
 - Rewrite: (no)
 - Mask: (111001111111)
- Syslog**
 - Enable syslog: (no)
 - Syslog facility: (DAEMON)
- Performance**
 - Threads: (2)
 - Sessions: (100000)
 - License warnings: (yes)
 - Virus warnings: (no)

ESET Mail Security

Kontrola odchozí / příchozí pošty, možnost nasazení na gateway

Úrovně použití:

1. **Postfix, Sendmail, Qmail, Exim – speciální agenti, tzv. Content filters**
2. **Transparentní kontrola SMTP, POP3, IMAP – agenti**
3. **Obecný modul esets_mda - testováno s mda procmail, maildrop, deliver, local.mail**

Široké možnosti konfigurace, dědění nastavení (domény/mailboxy)

Individuální parametry v rámci @domena, popř. uzivatel@domena.cz:



Volitelný zápis do záhlaví e-mailu, předmětu a hlavičky

Integrovaný antispam:

- Databáze IP adres, domén, e-mailových adres známých spammerů
- Sender ID Module – bayesián použit k identifikaci spammera na základě jeho minulých aktivit
- Analýza struktury zprávy (předmět, tělo, hlavička, použitá slova – spojení, obrázky...)
- SpamAdapt AI – automatické „učení“ Bayesiánského filtru

ESET File Security

Ochrana souborového systému serveru

Jednorázová kontrola na požádání, tj. on-demand – esets_scan

Rezidentní kontrola on-access dvěma metodami:

- Modul dazuko (esets_dac) www.dazuko.org
- preload libC knihovna – libesets_pac.so

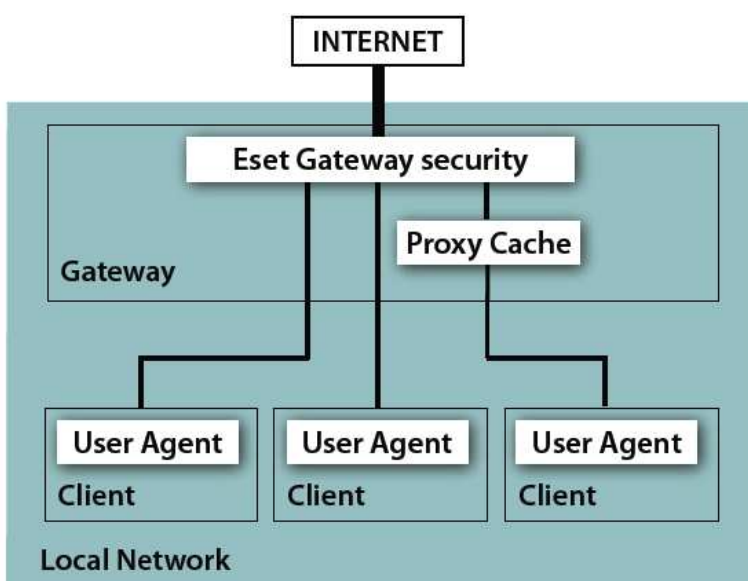
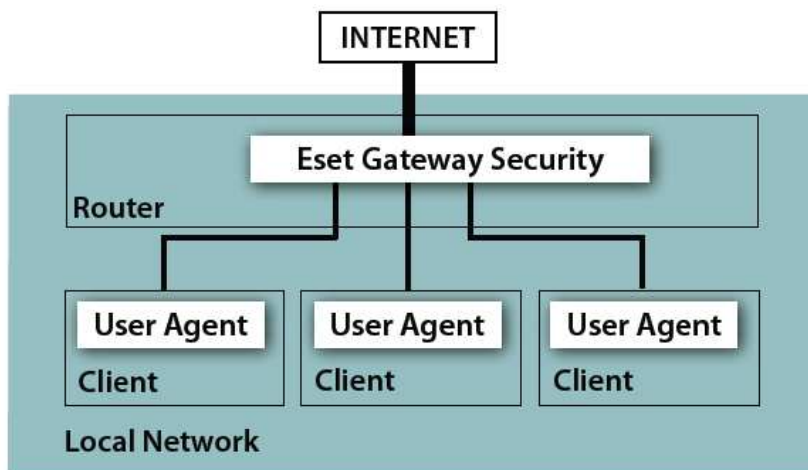
ESET Gateway Security

Kontrola komunikace / požadavků přímo na serveru – pro podnikový router - firewall

Transparentní kontrola síťových protokolů HTTP a FTP

- Na úrovni kernel IP routing
- Anebo na úrovni proxy (Squid Web Proxy Cache)

Speciální plug-in (esets_ssf.so) pro SafeSquid Proxy Cache



Linux jako Mirror server

Možnost využití Linuxového stroje jako Mirror server pro stanice Windows s NOD32 verze 2x

Jiná serverová řešení

- Založeny na ESET NOD32 generaci 2
- Spolupráce s NOD32 API
- Vyžadují licenční klíče

ESET NOD32 pro Exchange Server

Ochrana MS Exchange Serveru

Využívá VSAPI rozhraní společnosti Microsoft

Množství nabízených funkcí v závislosti na verzi ES

- podpora od verze 5.5, mazání celých e-mailů - 2003
- ochrana integrována do NOD32 Control Center jako modul XMON

„Stačí“ nainstalovat pouze NOD32 pro Exchange Server – zabezpečí i ochranu souborového systému.

Obsahuje NOD32 pro Windows v2 bez modulu IMON

Při instalaci je vyžadován LIC klíč (globální nastavení NOD32 Control Centra)

Možnost aktivovat Mirror /pro NOD32 v2/

ESET NOD32 pro Kerio

Plug-iny NOD32 jsou součástí přímo aplikací Kerio (Kerio Winroute Firewall, Kerio Mail Server)

komunikují s NOD32 API => nutné vlastnit příslušný LIC klíč (přidat přes NOD32 CC), každý produkt má svůj!

Na stejném stroji musí běžet NOD32 pro Windows v2

popř. NOD32 pro Linux Mail Server*

!	Doporučení
1.	expertní instalace NOD32 pro Windows – ZCELA ZAKÁZAT MODUL IMON
2.	v modulu AMON vyloučit přípony EML a TMP

NOD32 pro Lotus Domino

NOD32 (AMFE) jako Add-in, skenovací motor NOD32 verze 2.5

- podporuje Domino R5, R6, R6,5, R7
- před zahájením instalace (odinstalace) ukončit Domino server

Na stejném stroji musí běžet NOD32 pro Windows - LIC klíč (přidat přes NOD32 CC)

Funkce:

- Text přidávaný do infikovaných zpráv
- Pravidla pro filtrování zpráv
- Mazání infikovaných zpráv

NOD32 pro Novell Netware Server

Moduly AMON.NLM, NOD32.NLM, NOD32UPD.NLM

Instalace:

- nakopírovat do adresáře na Novellu
- zavést (LOAD) AMON.NLM a NOD32UPD.NLM
- autoexec.ncf

Aktualizace:

- neexistuje přímá aktualizace z Internetu

modul NOD32UPD.NLM pouze aktualizuje z jiného adresáře „on-fly“ = nutnost použití MIRROR z NOD32 v2.