STUDIJNÍ MATERIÁL PRO TECHNICKOU CERTIFIKACI
ESET Server Security, Serverové produkty

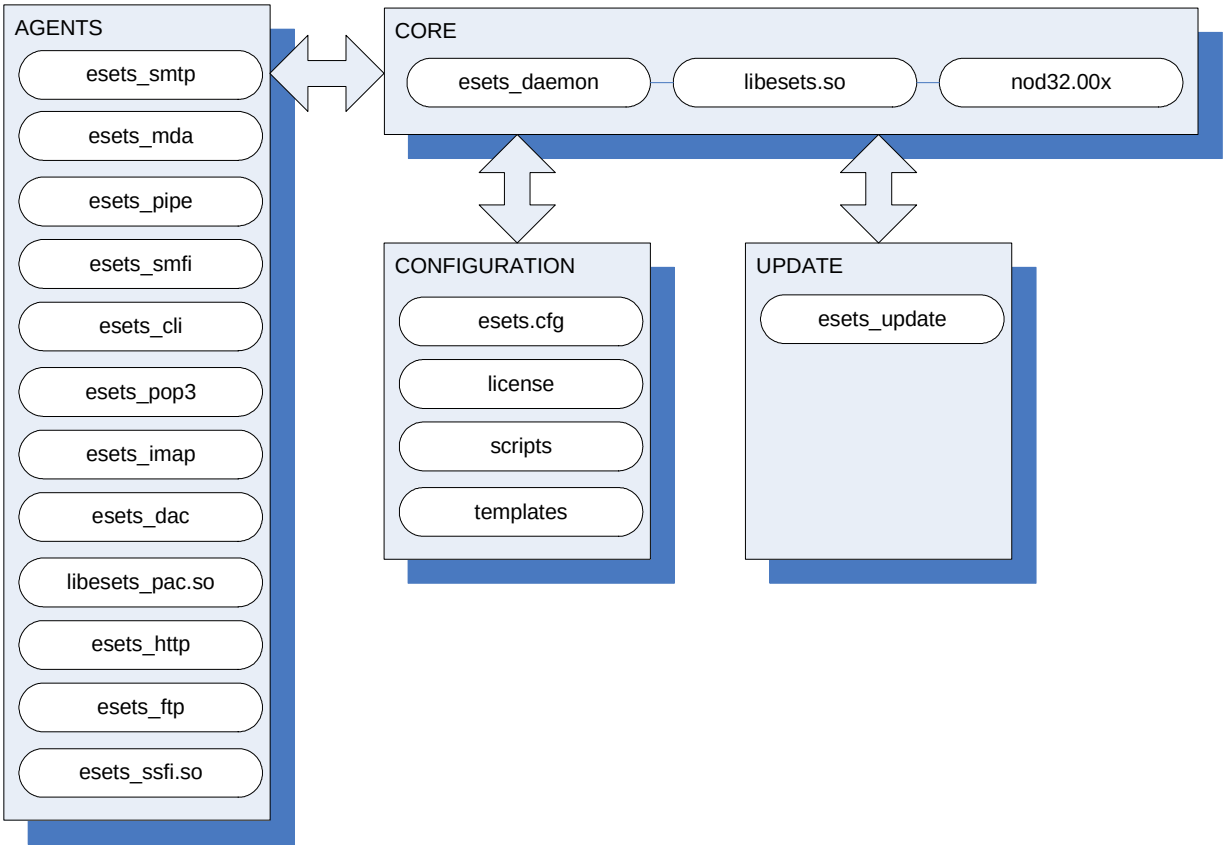
Eset software spol. s r.o., Meteor Centre Office Park, Sokolovská 100/94, 180 00 Praha 8
tel.: +420 233 090 233, fax: +420 233 090 230, obchod@eset.cz, www.eset.cz

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 můžou 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

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“ Bayesianského filtru

ESET File Security

Ochrana souborového systému serveru
Jednorázová kontrola na požádání, tj. on-demand – esets_scan

Rezidentní kontrola on-access dvěma metodami:

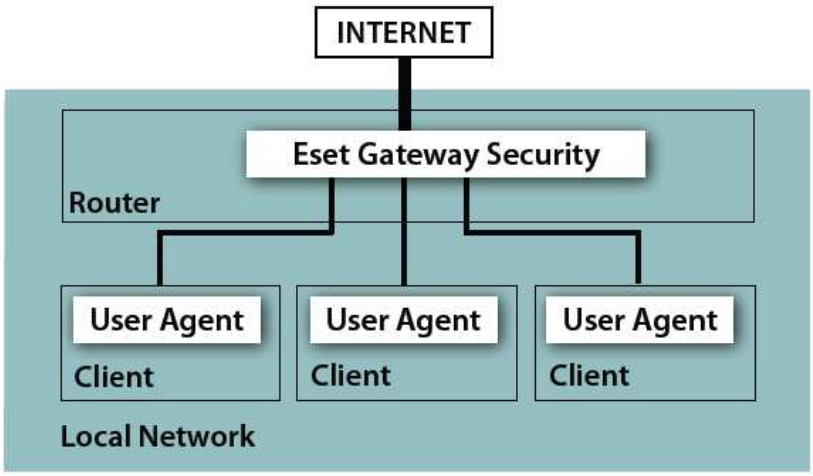
- Modul dazuko (esets_dac) www.dazuko.org
- preload libC knihovna – libesets_pac.so

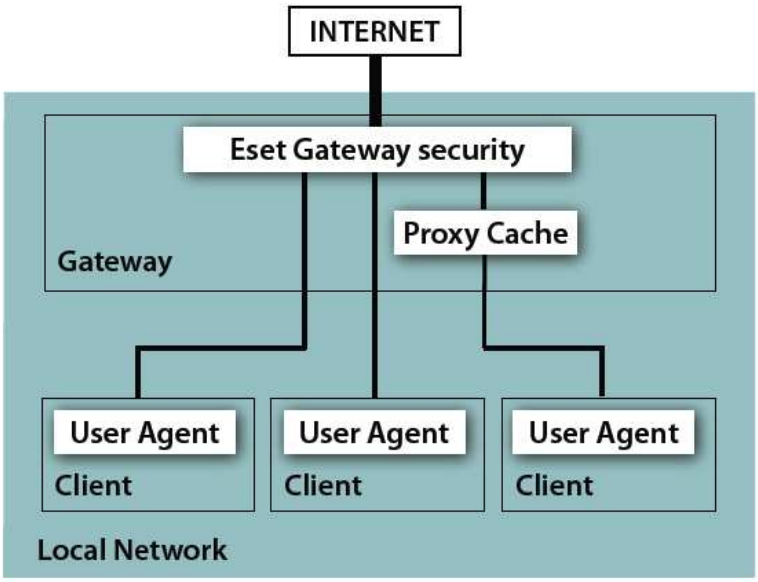
ESET Gateway Security

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_ssfi.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.