



*Produsele Business Kaspersky Lab sunt create pentru a proteja chiar și cele mai complexe și dinamice sisteme de rețea: produsele noastre includ suport pentru toate tipurile de noduri de rețea și platforme, precum și o scalabilitate avansată.*

## Solutii Mail Gateway

**activone.ro**



Kaspersky Mail Gateway este o soluție versatilă care furnizează protecție completă împotriva tuturor tipurilor de amenințări pentru utilizatorii sistemului de e-mail.

Kaspersky Antivirus pentru Linux Mail Gateway poate fi instalat pe un server separat și nu necesită integrarea în sistemul de e-mail existent. Soluția duce la creșterea semnificativă a nivelului de protecție împotriva amenințărilor informatice actuale, permițând utilizarea în aceeași rețea a soluțiilor antivirus dezvoltate de diferiți producători. De asemenea, protejează serverul de e-mail al companiei împotriva utilizării neautorizate.

Fiind destinată funcționării autonome, aplicația poate fi utilizată în orice mediu și se poate combina cu ușurință cu produse ale altor producători instalate pe alte noduri ale rețelei. Instalarea și configurarea sa nu necesită experiență vastă cu sistemele Linux.

### Funcții

- Protecție antivirus
- Filtrare adițională a mesajelor
- Control al accesului
- Administrare flexibilă
- Cerințe de sistem

### Protecție integrată împotriva programelor periculoase

**Scanare antivirus.** Programul scanează și îndepărtează orice tip de virus și alte programe periculoase sau potențial periculoase din toate elementele e-mailurilor primite și trimise, inclusiv atașamentele.

**Sistem de notificare a utilizatorului.** Dacă un obiect suspect sau infectat este detectat, administratorul de sistem, expeditorul și destinatarul mesajului vor primi un avertisment, al cărui conținut și format vor fi definite de administratorul de sistem.

**Carantină.** Obiectele infectate sau suspecte pot fi mutate într-un fișier tip carantină, unde administratorul poate să le vadă, să le șteargă sau să le trimită destinatarului final.

**Copii de rezervă.** Mesajele infectate pot fi salvate înainte de a fi procesate, făcând astfel posibilă restaurarea informațiilor importante dacă în procesul dezinfectare apar probleme.

## **Filtrare suplimentară a mesajelor**

**Filtrare după tipul atașamentului.** Aplicația poate fi configurată să filtreze traficul de e-mail după numele și tipul fișierului, ajutând la identificarea imediată a obiectelor ce pot conține viruși.

**Filtrare după grupul de utilizatori.** Administratorul poate defini reguli de procesare a mesajelor diferite pentru fiecare grup de utilizatori prin definirea limitărilor în conformitate cu politicile de securitate și nevoile angajaților.

## **Protecție a serverului împotriva accesului nepermis**

Aplicația poate fi configurată pentru a preveni atacurile de tip DoS și încercările neautorizate de utilizare a serverului pentru trimiterea de e-mailuri în masă. În unele cazuri acest lucru ajută la reducerea sarcinii serverului și mărește viteza de procesare a traficului de e-mail.

## **Administrare flexibilă.**

**Administrare de la distanță.** Kaspersky Anti-Virus for Linux Mail Gateway poate fi administrat de la distanță folosind o interfață web cât în modul tradițional, prin fișierul de configurare al aplicației.

**Configurarea și optimizarea aplicației.** În funcție de volumul traficului de e-mail și rigurozitatea politicilor de securitate ale companiei, administratorul poate schimba parametrii de operare ai aplicației, de la performanța maximă a sistemului la protecția maximă a utilizatorului.

Administratorul poate configura și anumite intervale de trimitere și/sau primire a mesajelor, poate coordona lista de așteptare și poate limita numărul obiectelor care pot fi scanate în mod simultan în modul plan secund.

**Configurarea actualizărilor.** Semnăturile amenințărilor și modulele programelor pot fi actualizate la cerere sau automat pe baza unui program prestabilit de pe serverele Internet ale Kaspersky Lab sau de pe serverele locale specificate de administratorul de sistem.

## **Cerințe hardware :**

Procesor din clasa Intel Pentium (recomandat Pentium III sau Pentium IV)

Cel puțin 256 MB de RAM

cel puțin 100 MB spațiu disponibil pe disc pentru instalare

Cel puțin 500 MB disponibili în sistemul de fișiere temporare

## **Cerințe software :**

### **Pentru platformele de 32-bit:**

- Red Hat Enterprise Linux Server 5.
- Fedora 7.
- SUSE Linux Enterprise Server 10.
- OpenSUSE Linux 10.3.
- Debian GNU/Linux 4 r1.
- Mandriva 2007.
- Ubuntu 7.10 Server Edition.
- FreeBSD 5.5, 6.2.

**Pentru platformele de 64-bit:**

- Red Hat Enterprise Linux Server 5.
- Fedora 7.
- SUSE Linux Enterprise Server 10.
- OpenSUSE Linux 10.3.

**Perl** versiunea 5.0 sau mai mare ([www.perl.org](http://www.perl.org))

Which

Bzip2

**Programul Webmin** versiunea 1.070 sau mai recentă ([www.webmin.com](http://www.webmin.com)) pentru administrare la distanță (opțional)