



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 Anti-Virus pentru Proxy Server

activone.ro



Kaspersky Anti-Virus for Proxy Server protejează întregul trafic Internet HTTP și FTP care trece prin serverul proxy .

Aplicația asigură securitatea utilizatorilor atunci când lucrează online și șterge programele periculoase și viermii care se răspândesc prin intermediul programelor de mesagerie instant .

Funcții

- Protecție antivirus
- Administrare flexibilă
- Cerințe sistem

Protecție împotriva virușilor, Troienilor și programelor de tip spyware

Scanare în timp real a traficului Internet. Programul detectează și șterge toate tipurile de viruși, viermi, Troieni și alte programe periculoase din traficul care trece prin majoritatea tipurilor de servere proxy.

Alegere a parametrilor de filtrare. Programul include o gamă largă de parametri de filtrare (adrese IP și URL-uri, tipuri MIME și mărimea fișierului), care pot fi folosiți la crearea regulilor individuale de scanare pentru grupuri diferite de utilizatori

Scanare a fișierelor arhivate. Kaspersky Anti-Virus furnizează cea mai bună detecție a virușilor, din orice tip de fișier sau atașament. Programul este compatibil cu mai mult de 70 de formate de arhivare (peste 240 de versiuni) și cu mai mult de 260 de tipuri de fișiere comprimate (peste 1330 de versiuni).

Detectare a programelor cu potențial periculos. Folosind opțiunea de protecție extinsă, aplicația poate detecta și șterge nu numai programe periculoase cunoscute, dar și pe cele cu potențial ostil (cum sunt programele de tip spyware).

Administrare flexibilă

Administrare de la distanță. Aplicația poate fi administrată de la distanță, prin interfața web, sau printr-un singur fișier de configurare

Politici de securitate la nivelul grupului. Administratorul poate seta reguli individuale de filtrare a traficului pentru fiecare grup de utilizatori, ceea ce definește privilegiile în conformitate cu politica de securitate a companiei și cerințele angajaților.

Sistem de notificare a utilizatorului. Programul blochează, în mod automat, orice obiect infectat și trimite utilizatorului o notificare în format HTML. Administratorul de sistem poate configura conținutul, forma și limba notificărilor.

Sistem de rapoarte și statistici. Aplicația poate realiza rapoarte statistice pentru a ajuta administratorul să urmărească activitatea virușilor și să monitorizeze performanța aplicației.

Module de actualizare configurabile. Actualizările bazei de date antivirus și a modulelor programului sunt disponibile la cerere, în mod automat sau pe baza unui program prestabilit. Pot fi descărcate direct de pe serverele de Internet Kaspersky sau de pe serverele locale ale companiei.

Încredere crescută. Protecția împotriva scurgerilor de informație din memorie, conflictele hardware, erori de input/output și conflicte critice de sistem asigură o performanță rapidă și stabilă a aplicației.

Cerințe hardware :

Configurație minimă (10 sau mai mulți utilizatori, aproximativ 20 de solicitări pe minut cu dimensiune medie de 15 KB):

Procesor din clasa Intel Pentium

Cel puțin 64 MB RAM

Cel puțin 200 MB spațiu liber pe disc pentru stocarea fișierelor temporare și cel puțin 50 MB spațiu liber pe disc pentru instalare

Configurație recomandată:

50 sau mai mulți utilizatori, trafic de 256 MB pe zi, o medie de 20 de cereri pe minut, maxim 900 cereri pe minut, RAM utilizat de aplicații în momente de vârf: 64 MB:

Procesor Pentium II 300

Cel puțin 128 MB RAM

Cel puțin 512 MB spațiu liber pe disc pentru stocarea fișierelor temporare și cel puțin 50 MB spațiu liber pe disc pentru instalare

250 sau mai mulți utilizatori, trafic 1 GB pe zi, o medie de 150 cereri pe minut, maxim 1300 cereri pe minut, RAM utilizat de aplicații în momente de vârf 128 MB:

Procesor Pentium IV

Cel puțin 256 MB RAM

Cel puțin 1 GB spațiu liber pe disc pentru stocarea fișierelor temporare și 50 MB spațiu liber pentru instalare

Cerințe software :

Unul din următoarele sisteme de operare:

Platforme de **32-bit**:

Red Hat Enterprise Linux Advanced Server 4 Update4

Fedora Core 6

SUSE Linux Enterprise Server 10

SUSE Linux Enterprise Desktop 10 (only for Workstation)

openSUSE Linux 10.2

Debian GNU/Linux 3.1 updated (r4)

Mandriva 2007

FreeBSD 5.5, 6.2

Platforme de **64-bit**:

Red Hat Enterprise Linux AS/ES 4

Fedora Core 6

SUSE Linux Enterprise Server 10

openSUSE Linux 10.2

FreeBSD 6.2

Unul din următoarele servere proxy :

Squid (compatibil cu protocolul ICAP)

Blue Coat SG Appliance

NetApp/Blue Coat NetCache

Cisco ACNS Content Engine

Utilitarul which

Pachetul Webmin (opțional) – pentru administrarea la distanță a aplicației

Perl 5.0 sau mai recent (www.perl.org)