KinderGate Parental Control is a tool designed for educational institutions and home users to control Web resources used by students or children.

Dangerous contacts
Websites about drugs
Websites for adults
Websites with viruses

ONLINE PROTECTION for your family

www.kindergate-parental-control.com | sales@entensys.com
KinderGate Parental Control Features

HTTPS Traffic Filtering
Alongside ordinary unencrypted traffic, KinderGate Parental Control can be configured to filter HTTPS traffic. The server performs certificate-swapping and morphological filtering on the fly.

Safe Search
KinderGate Parental Control features “Safe Search” function that helps block unwanted requests, such as pornography, swearwords, etc. in Google, Yahoo and other search engines. "Safe Search" blocks not only websites but video and pictures as well.

Files Download Control
KinderGate Parental Control can prevent your child from downloading unwanted files (EXE, DOC, MP3, AVI, etc.). For example, archived files often contain trojans, and video content may not correspond to its title. Also you can choose what type of files downloads you would like to block.

Block Unwanted URL Categories
With KinderGate Parental Control, parents can deny access to web sites with adult content and block a wide range of other URL categories, including resources containing malicious software, web sites related to drugs and violence, gaming resources, etc. The tool can also monitor categories of web pages visited by your child without denying access to any resources.

Statistics
The Statistics page is used to collect, view, and update statistics on Internet use by the number of network requests and responses to network requests. Information on the number and type of outgoing network requests has the following status:
- Blocked
- Allowed
- Ad block requests.

Deep Content Inspection (DCI)
KinderGate Parental Control features Deep Content Inspection function that enables a better protection from unwanted online factors.

Deep Content Inspection is a network filtering feature that examines actual content instead of examining individual or multiple packets.

Using Morphological Analysis mechanism, Deep Content Inspection checks a web page for unwanted content. Morphological Analysis provides intelligent filtering with most popular languages morphology support, this way KinderGate examines content not only for certain word groups but their different variations as well. You can enable the feature to check for such categories, as “Bad Words”, “Drugs”, “Suicide”, “Terrorism”, “Pornography”, “Gambling”.

Clustering support
KinderGate Parental Control features clustering support which allows creating a system of several machines that is controlled and operated from the same computer. The cluster consists of a node, nodes replicate settings and their local cache with all the remaining nodes in the cluster. Information on all user requests is stored locally on each server (raw data) and it is not replicated on other servers.

Instructions for installing KinderGate in cluster are available in User’s Guide.

Block Dangerous Websites
The Internet becomes more dangerous environment every day. With KinderGate, you may block access to over 500 million websites that feature phishing, Trojans, keyloggers, botnets and other malicious software. The database of dangerous websites is updated on a daily basis. One more feature is the contextual advertisement filter that you can enable in the web surfing settings. It will keep children away from unwanted resources and become a valuable tool for parents, as it blocks annoying banners that pop up on numerous websites.

Statistics
The Statistics page is used to collect, view, and update statistics on Internet use by the number of network requests and responses to network requests. Information on the number and type of outgoing network requests has the following status:
- Blocked
- Allowed
- Ad block requests.

System requirements:
Windows XP/ 2003/ 2008/VISTA/ 7 (X32, X64)
MAC OS 10.7.5, ALT LINUX/UBUNTU
Option of run on virtual machine!