Complex Internet filtering for educational institutions

Working with web resources is inextricably linked with the risk of encountering online threats. This problem is a particular issue for colleges and K-12 schools. On the one hand, teachers and lecturers can use the web as part of their teaching to make classes more interesting for students, but on the other hand, it can lead to pupils viewing content that is unsuitable for children, violating a whole range of national and international legislation, such as the Children’s Internet Protection Act (CIPA) and Internet Watch Foundation (IWF). Besides this, viruses on harmful sites can become a real headache, not only for the network managers that maintain the institution’s network, but also for all of the teaching staff.

Filtering mechanisms of Entensys solutions

Entensys has been working on Internet censorship for more than 10 years, incorporating the very latest technology into our products and paying special attention to legislative requirements. The web resource filtering system developed by Entensys specialists uses mechanisms to analyze content:

- **Category-based filtering** (Entensys URL Filtering 2.0) – URL filtering using enormous base containing 500M+ websites which are divided into 70+ categories (pornography, social networks, drugs, etc.).

- **Blocking banners and pop-ups** – blocking of advertisement on all websites in order to avoid clicking undesired links accidentally and malicious content.

- **Morphological analysis** – checking web pages content for certain words and phrases.

- **Safe search** – blocking of undesirable content at request level in search engines Google, Yandex, Bing, Rambler.

- **Black and White lists** – web pages filtering by reference to their presence/absence in lists.

- **Control of downloading files** – The feature prevents from downloading unwanted files (EXE, DOC, MP3, AVI, etc).

- **HTTPS Traffic Filtering** – Filtering and analyzing encrypted HTTPS protocol, using the same filtering mechanisms as for unencrypted traffic.

IT classrooms with public Internet access (including libraries) are also used by pupils outside of classes. In these situations, in addition to other threats, the risk of undesirable online friendships arises, which may sometimes lead to child harassment by fraudsters or pedophiles.

The increase in the number of online threats imposes a new demand on educational institutions – their ability to provide child security in cyberspace. The optimal solution to this issue is implementing an effective Internet filtering system. Administrators in K-12 schools, where no Internet censorship is currently installed, risk to be accused by parents. In some countries, failure to install Internet filtering in educational institutions can lead to administrative and criminal liability.

**Uncontrolled Internet access for kids in educational institutions is:**

- Malicious websites
- Undesirable contacts
- Pornography resources
- Harmful information
- Cheats and pedophiles

**School, college**

- Parents’ disaffection
- Doubtful reputation of institution
- Virus infection danger

www.entensys.com | sales@entensys.com
Blocking of websites and material restricted at a national level

The problem of child security on the Internet has reached an international scale. In many countries this issue is regulated by government bodies. In most cases, the state imposes a ban on specific websites and material. Similar lists can easily be developed for K-12 schools using the “Black and white lists” and “Morphological analysis” mechanisms.

Entensys solutions include the ability to import lists of websites and dictionaries, as well as editing existing ones. From the developer’s point of view, an automatic black list update mechanism is included, containing resources in different languages and relevant to the majority of countries in the world. Entensys web filters currently include prepared dictionaries for “suicide”, “terrorism”, “pornography”, “bad words” and “drugs” in English, French and German.

Benefits of the Entensys filtering package

- High level of effectiveness (99.8% of harmful sites**)
- Low false response level (less than 0.6%)
- Flexible settings
- Complies with a multitude of security policies
- Unique approach to different types and groups of content (video, images, photos, text, etc.)
- Web 2.0 content filtering
- Secure working for students in K-12 schools, colleges and libraries

Implementation options

At provider level

The filtering system can be implemented at Internet Service Provider level. To make the integration process more convenient, Entensys has developed a special API for UserGate Web Filter. The option of clustering this solution allows you to roll out the filtering system on providers’ systems of any scale serving K-12 schools.

At Internet gateway level

UserGate Web Filter provides safe web surfing at an Internet gateway level. This avoids the need to install and configure the filtering system on each computer in the school or college individually.

At personal computer level

KinderGate Parental Control is installed and configured on each machine in the educational institution’s IT suite.

ENDENSYS: CONNECT. PROTECT. MANAGE!